imation

DataGuard Appliances

USER MANUAL

Imation Product Support

If you experience problems with setup and/or use of your new DataGuard Appliance, please review this product manual or visit http://www.imation.com and click on the support link.

For the DataGuard Appliance Compatibility Guide, go to:
https://support.imation.com/app/answers/detail/a_id/220

For DataGuard Appliance Rack Mount Instructions, go to:
https://support.imation.com/app/answers/detail/a_id/221

Your DataGuard Appliance should now be operating smoothly—and we want to help you keep it that way. For the fastest product support and the latest drivers and downloads, register your DataGuard Appliance today at register.imation.com.

Limit ed Warranty: If any defect in material or manufacture appears within 3 years of the date of original purchase of this product, it will be replaced or the purchase price refunded. For more information, go to www.imation.com. This warranty does not apply to normal wear or damage from misuse, abuse or accident. Imation will not be liable for any lost data or other indirect, incidental or consequential damages. This warranty gives you specific rights—you may have other rights that vary from country to country.

FOR SALES IN AUSTRALIA: Imation Limited Warranty against defects for 3 years from purchase date. Product will be replaced or refunded at our option. At your cost, deliver product & proof of purchase to Imation at Unit 2, 1 Coronation Ave, Kings Park NSW, Australia 2148 Ph 1800 225 013. Further details at www.imation.com/en-au or contact us at csanz@imation.com.

Your benefits under this Imation warranty are in addition to your other rights and remedies under a law in relation to this product. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Imation and the Imation logo are trademarks of Imation Corp. RDX is a registered trademark of Tandberg ASA. All other trademarks are the property of their respective owners.

© Imation Corp
Imation Enterprises Corp 1 Imation Way Oakdale, MN 55128-3414
63951337-B

Important Safety Instructions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Note: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This Class A digital apparatus complies with Canadian ICES-003.

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
13. Unplug this apparatus during lightning storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

Specifications

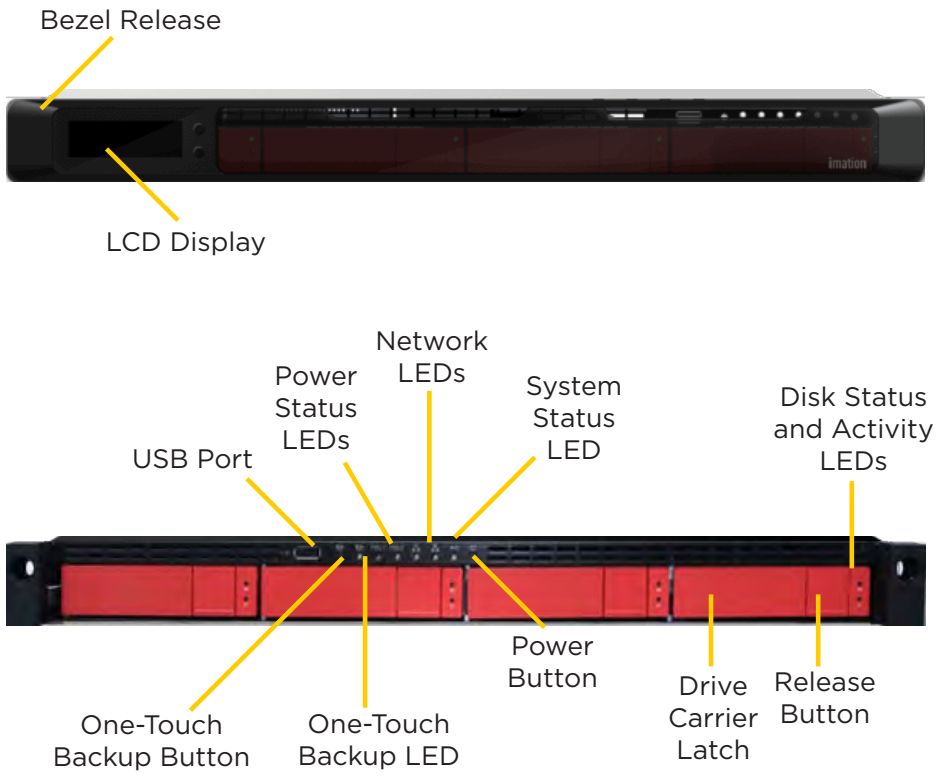
Processor	Intel® Atom™ Processor D2700, 2.13GHz
Memory	2GB DDR3 RAM
HDD Type	3.5" 3Gb/s SATA
Number of HDD	Up to 4 HDD (R4) • Up to 5 HDD (T5R)
Power Supply	2 x 250W (R4) • 1 x 250W (T5R)
Power Management	Power scheduling on/off; wake-on-LAN; HDD spin-down; MAID 2.0
UPS Support	USB / Ethernet
Ethernet	2 x Gigabit Ethernet ports
USB	(2) USB 3.0 ports • (3) USB 2.0 ports
eSATA	1 x eSATA
RAID Levels	0, 1, 1E, 3, 5, 6, 10
RAID Functions	Drive roaming, robust error handling, RAID level migration, online capacity expansion, PDM, media patrol, synchronization
Protocol Support	TCP/IP, SMB/CIFS, HTTP/HTTPs, FTP, NFS, WebDAV, AFP, SNMP, SSH, Telnet, LLTD, DHCP (Server/Client), IPV4, IPV6, DDNS
Account Management	Supports Microsoft ADS (Active Directory Services)
Operating Systems	Supports Windows XP, Vista, 7, Server 2003, Server 2008, Server 2008 R2, Linux/Unix 2.6 Kernal or above, Mac OS X 10.4 or above.
File System	XFS
External Storage Support	EXT3, FAT32, XFS, HFS+, NTFS
System Management	• DataGuard Management Interface (AJAX 2.0, Web-based) • Supports multi-language interface, including English, Traditional Chinese, Simplified Chinese, Japanese, Korean, German, French, Italian, Spanish, Portuguese, Russian • CLI (command line interface) • Email alert; advanced system log • System firewall and concurrent connection monitor • Firmware upgradable > new firmware notice and upgrade
iSCSI	Supports iSCSI target service and capacity expansion
Backup Options	Snapshot, replication, Amazon S3 support, DropBox, OpenStack, RDX, external storage backup (one-touch backup)
Dimensions	44.5mm H x 445mm W x 495mm D (R4) 254mm H x 188mm W x 243mm D (T5R)

Caution
The electronic components within the device are sensitive to damage from electro-static discharge (ESD). Observe appropriate precautions at all times when handling this device or its subassemblies.

Front Panel—R4

The front panel provides access to the hard drive carriers, power button, and one USB 2.0 connection (USB Port 1). The bezel (not shown) includes an LCD display.

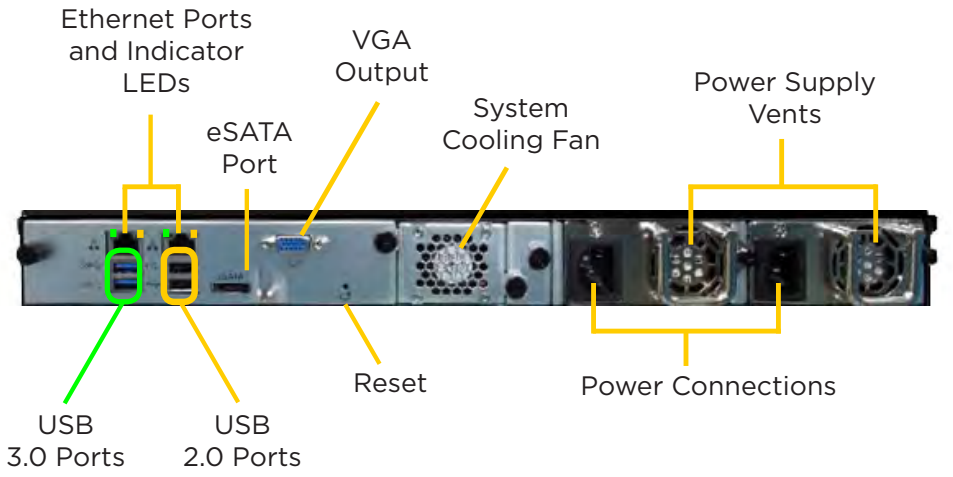
Feature	Description
Network LEDs	Indicators flash when network connection is active.
USB Port	Supports USB 2.0 for One-Plug-Auto-Service (OPAS), USB printer, external USB hard drive or USB uninterruptable power supply. This port is labeled USB1 in the Management Interface.
LCD Display and Controls	Displays name and IP address for the device. Use with the Select and Enter buttons to view critical system statistics or configure the IP address. (On front bezel; not shown)
One-Touch Backup Button and LED	Initiates data backup for a client system with backup schedule configured. When the button is pushed, the LED below flashes amber; during backup, it blinks green; when the backup is complete, a buzzer sounds once.
Disk Status LED	Upper indicator glows green when the disk is functioning normally, amber when the disk is rebuilding, and red if the disk has failed.
Disk Activity LED	Lower indicator flashes blue to show read/write activity.
Power Button and Status LED	Button powers DataGuard Appliance on and off. Status LED on power button glows green when the power supply is functioning normally, and amber in case of a critical disk error.
Release Button	Allows user to release drive carrier from chassis.
Drive Carrier Latch	Lets user remove released carrier for installation or replacement of hard drive.



Back Panel—R4

The back panel contains power and network connections, maintenance features and cooling vents.

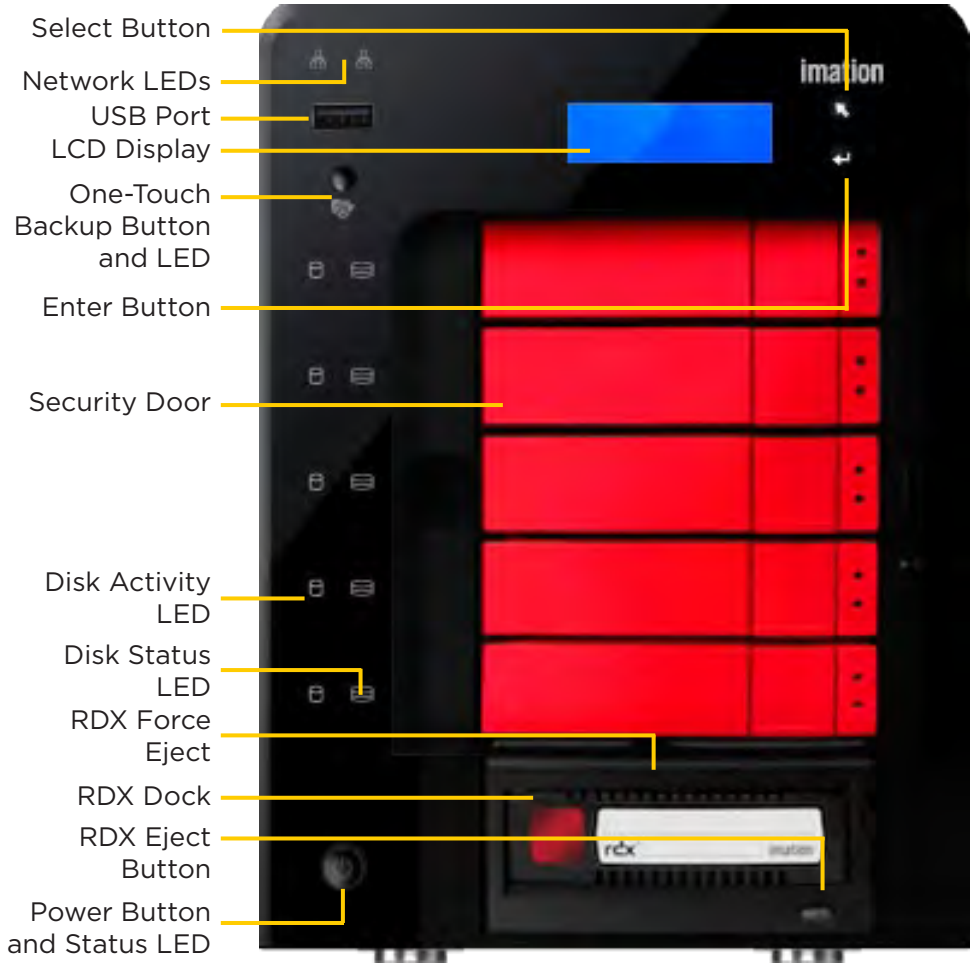
Feature	Description
Ethernet Ports and Indicator LEDs	Allows connection to a LAN or dedicated storage network or subnet. The LED at the left of each port glows briefly when a link is established, and blinks when the port is being used. The LED at the right of each port glows green at 1000 Mbps and amber at 100 Mbps. At 10 Mbps, the indicator does not illuminate.
eSATA Port	Provides connection to external SATA storage.
VGA Output	Lets a qualified technician or engineer connect a VGA monitor for managing the system out-of-band. Should only be used for diagnostics and technical support.
System Cooling Fan	Provides air cirulation to system and keeps drives from overheating. Leave several inches of space behind this opening.
Power Supply Vents	Provide air cirulation to power supplies. Do not block.
USB Ports	Connections are numbered 1–5 for reference in the Management Interface. Ports 2–3 (lower and upper left) support USB Specification 3.0. Ports 4–5 (lower and upper right) support USB Specification 2.0. Port 1 is on the front panel.
Reset	Lets an administrator perform a hardware reset.
Power Connections	Accepts one cord for each power supply. Use the cord shipped with the device and connect it to a suitable power source.



Front Panel—T5R

The front panel provides access to the hard drive carriers, RDX cartridge, power button, one USB 2.0 connection (USB Port 1) and LCD display.

Feature	Description
Network LEDs	Indicators flash blue when network connection is active.
USB Port	Supports USB 2.0 for One-Plug-Auto-Service (OPAS), USB printer, external USB hard drive or USB uninterruptable power supply. This port is labeled USB1 in the Management Interface.
LCD Display and Controls	Displays name and IP address for the device. Use with the Select and Enter buttons to view critical system statistics or configure the IP address.
One-Touch Backup Button and LED	Initiates data backup for a client system with backup schedule configured. During backup, the LED below illuminates; when the backup is complete, a buzzer sounds once.
Disk Activity LED	Indicator flashes blue to show read/write activity.
Disk Status LED	Indicator glows blue when the disk is functioning normally, amber when the disk is rebuilding, and red if the disk has failed.
RDX Dock	Accepts any RDX cartridge. Read manual for RDX system before using. LED on eject button glows green when RDX cartridge is installed, and flashes amber when the cartridge is being ejected.
Power Button and Status LED	Button powers DataGuard Appliance on and off. Status LED on power button glows blue when the power supply is functioning normally, red during initialization, and amber in case of a critical disk error.

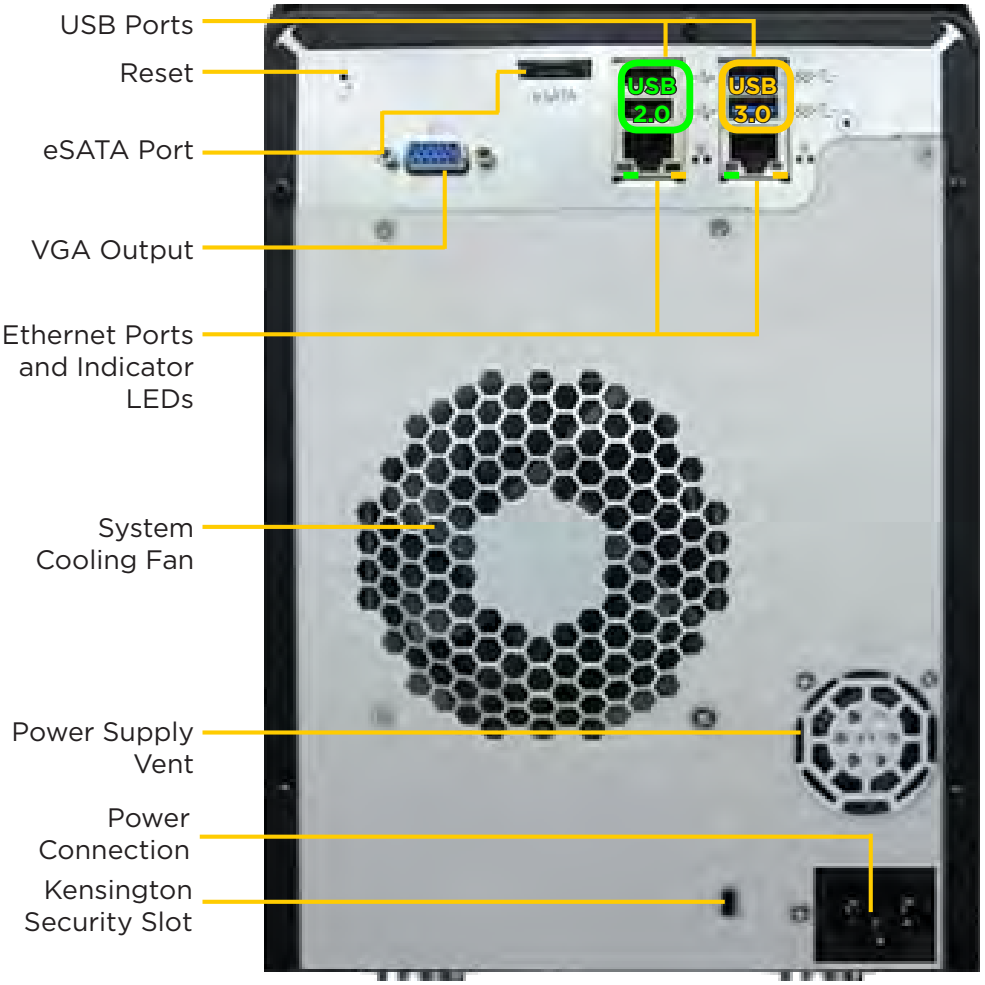


T5R Front Panel View (door closed)

Back Panel—T5R

The back panel contains power and network connections, maintenance features and cooling vents.

Feature	Description
Reset	Lets an administrator perform a hardware reset. See page 8 for details.
eSATA Port	Provides connection to external SATA storage.
USB Ports	Connections are numbered 1–5 for reference in the Management Interface. Ports 2–3 (upper and lower right) support USB Specification 3.0. Ports 4–5 (upper and lower left) support USB Specification 2.0. Port 1 (USB 2.0) is on the front panel.
Ethernet Ports and Indicator LEDs	Allows connection to a LAN or dedicated storage network or subnet. The LED at the lower left of each port glows briefly when a link is established, and blinks when the port is being used. The LED at the lower right of each port glows green at 1000 Mbps and amber at 100 Mbps. At 10 Mbps, the indicator does not illuminate.
VGA Output	Lets a qualified technician or engineer connect a VGA monitor for managing the system out-of-band. Should only be used for diagnostics and technical support.
System Cooling Fan	Provides air cirulation to system and keeps drives from overheating. Leave several inches of space behind this opening.
Power Supply Vent	Provides air cirulation to power supply. Do not block.
Power Connection	Use the cord shipped with the device and connect it to a suitable power source.
Kensington Security Slot	Allows user to add physical security to the device.



T5R Rear Panel

Installing Hardware

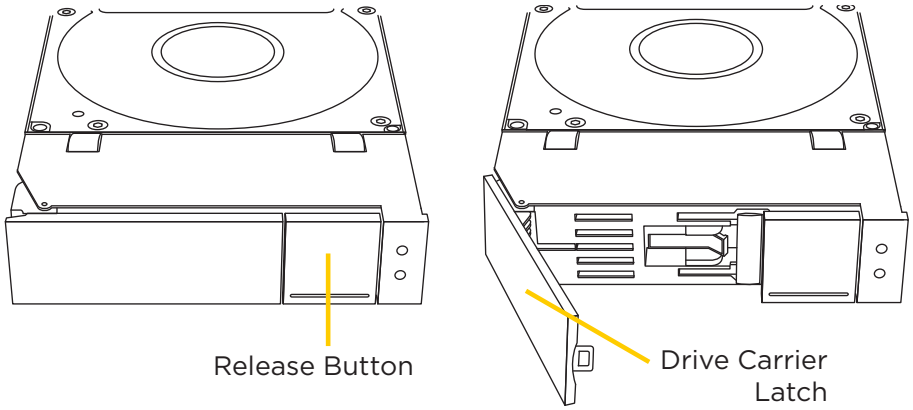
Follow the instructions below to install hard disk drives, connect the Data Guard Appliance to the network, and power it on. If your DataGuard Appliance shipped with hard drives already installed, use these instructions for replacing a hard drive.

Unlock and Open Security Door (T5R Only)

Using the key included, unlock the security door and open it completely.

Remove Drive Carrier

1. Press the square button on the right side of a drive carrier. This will release the latch on the left side.Hold the latch and gently pull the carrier out of its slot. It is now ready to receive a new drive.



Warning
To avoid direct contact with electrical hazards and possible injury, remove only one drive carrier at a time.

Place New Drive in Carrier

1. Place the empty drive carrier on a table or other stable platform. Orient the drive so that the SATA contacts and power connector will face the rear of the enclosure (Figure 1). Place the drive in the carrier so that the screw holes are aligned.
2. Fasten the drive to the carrier using only the counter-sink screws provided (Figure 2). Use four screws per drive and be careful not to over-tighten them.

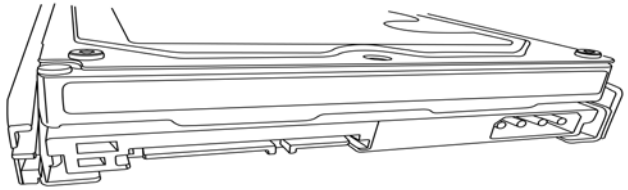


Figure 1

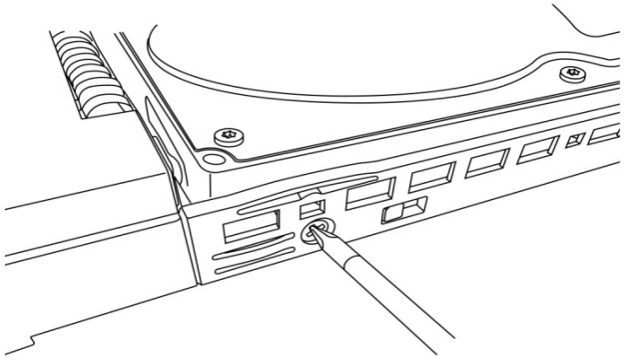


Figure 2

Important
To achieve the best data protection, select enterprise level, SATA 3.0 Gb/s drives. For optimal performance, install drives of the same model, speed and capacity.

Insert Assembled Carrier into Empty Bay

With the hard drive securely fastened to the carrier, it can be inserted into an empty bay on the DataGuard Appliance. Follow these steps:

1. Pick up the assembled drive carrier.
2. Slide the carrier most of the way into the empty bay.
3. With a fingertip, push against the right side of the carrier until it is flush with the other carriers.
4. Press the latch to secure the carrier. The power and interface connectors will engage when the latch is closed correctly.

To install additional hard drives, follow these same directions for each drive bay.

Connect DataGuard Appliance to Network

After one or more drives have been installed, the DataGuard Appliance can be placed on a network. Using the included Ethernet cable or an equivalent, establish a network connection by following these steps:

1. Insert an Ethernet cable (Category 5e or better) into either RJ45 port on the rear panel.
2. Insert the other end of the cable into the RJ45 port on a networked Ethernet switch or similar device.
3. When the device is powered on and a link is established, two indicators will glow: a green LED next to the lower right corner of the connected Ethernet port, and the link indicator on the front panel.

Power On DataGuard Appliance

1. Attach the included power cord to the power connection on the rear panel.
2. Connect the power cord to a suitable power source.
3. Press the power button on the front panel. The device will boot up and conduct a routine self-test. When the system is fully booted, the status LED will glow.
4. Shut Down DataGuard Appliance

To shut down the DataGuard Appliance, press and hold the Power button for about 8 seconds. The Status LED will turn red, then go dark. You can also reboot or shut down the device by using the LCD display controls, or over a network with the DataGuard Management Interface. To restart, press the power button again.

Visible and Audible Alerts

Audible Alarm

The DataGuard Appliance has two beep patterns.

- **One beep**, not repeated: The DataGuard Appliance is online
- **Two beeps**, continuously repeated: The DataGuard Appliance is reporting a problem

When you boot or reboot the DataGuard Appliance, and the buzzer is enabled, the buzzer sounds once to indicate that the DataGuard Appliance is online.

System Status LED

The system status LED reports the condition of the enclosure fan and power supply:

- **Blue:** Normal Enclosure function
- **Amber:** There is a problem with the fan or power supply
- **Red:** The fan, power supply, or file system has failed.

The system status LED blinks red three times when you click the **Locate** button in the DataGuard Management Interface. If your DataGuard Appliance is configured to work with a UPS, it will continue to run after a power supply failure.

Disk Status LEDs

The disk status LEDs report the condition of the hard drives:

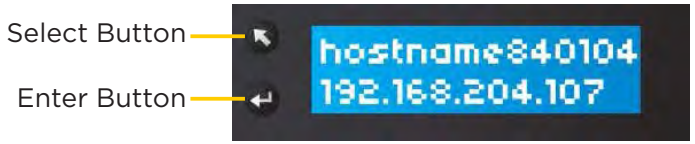
- **Blue**: Normal disk drive function
- **Amber:** Rebuilding to this disk drive
- **Red:** Failed disk drive
- **Dark:** No disk drive is installed

Disk status LEDs are also dark when the drives are powered down during system stand-by.

Hardware Reset

A hardware reset will clear the flash memory of the device: the User Name, Password, IP Settings, user account settings, and other administrative configuration settings will be set to factory default. A hardware reset will not change RAID configurations or any array or logical drive arrangement.

After a hardware reset, reboot the system and configure the system using the default User Name “administrator” and default Password “password”.



Use LCD Panel Controls

The LCD display and controls on the front panel let you monitor vital system statistics, check the firmware version, configure IP settings, and reboot or shut down the device. To review system status, press the Select button repeatedly. The display will cycle through these nine categories of system information:

- 12V Voltage
- 5V Voltage
- 3.3V Voltage
- CPU Temperature
- Fan Speed
- System Date
- System Times
- Firmware Version
- BIOS Version

After the BIOS Version is displayed, you can choose from two options:

- Press the Select button once more to display the “Back to Main Page” option
- Press the Enter button to return to the device name and IP address

Configure Network Settings

When the DataGuard Appliance is first connected to an active network, it will retrieve an IP address automatically. A fixed (static) IP address is recommended. If possible, specify a fixed IP address through the LCD panel by following these steps:

1. Press Enter once. The display will show “Network Setting Enter?”
2. Press Enter again. The display will show “Network Setup”, “DHCP” and “Fixed”.
3. Press Select to switch between DHCP and Fixed; press Enter to confirm your selection.

✓ If you choose DHCP, the display will show the options “Cancel” or “OK”. Press Select to switch between these two options, then press Enter to confirm your selection.

✓ If you choose Fixed, the display will show the current IP address with the first digit highlighted. Press Select until this digit shows the number you want, then press Enter to confirm your selection and move to the next digit.

✓ When all numbers are set, press Enter. The display will show the options “Cancel” or “OK”. Press Select to switch between the two options, then press Enter to confirm your selection.

✓ Follow the same procedure to set a Gateway address, then press Enter to confirm your selection.

Set Display Language

1. When the display shows the IP address, press Enter. The LCD will show “Network Setting Enter?”
2. Press Select once. The LCD will show “Display Language”.
3. Press Enter to change the current display language.
4. Press Select to cycle through the available languages, then press Enter to confirm your selection.

Set Power Control Functions

1. When the display shows the IP address, press Enter. The LCD will show “Network Setting Enter?”
2. Press Select twice. The LCD will show “Power Control Enter?”
3. Press Enter once. The LCD will show “Shutown/Reboot” above and “Shut Down?” below.
4. To switch between these options, press Select; to confirm your selection, press Enter.
5. The LCD will show “Cancel” and “OK”.
6. To switch between these options, press Select; to confirm your selection, press Enter.

RDX Dock and Cartridges—T5R

The T5R has a built-in RDX dock that provides additional capabilities for data management. You can use RDX cartridges to make secondary backups for off-site storage, transfer large data sets to and from the DataGuard Appliance, or seed an online cloud system. All functions are controlled through the DataGuard Management Interface. Follow these directions when using RDX cartridges.

Handling RDX Cartridges

Although RDX cartridges are rugged, take care not to drop them. This will ensure data integrity and long life. Also observe the following precautions:

- Store cartridges in their protective cases when you are not using them; do not stack RDX cartridges.
- Keep cartridges away from dust, dirt, moisture, direct sunlight, heat sources and temperature extremes or rapid changes in temperature.
- Never try to force a cartridge into the dock. If it is difficult to insert, check the orientation and ensure correct alignment using the keyed corner as a guide (see Figure 1).

Loading and Unloading Cartridges

The RDX dock in each T5R has a cartridge slot with a hinged protective door, and a power indicator that also functions as a cartridge eject button. Cartridges only fit in one orientation (see Figure 1).

- To load a cartridge, orient its keyed corner to the upper left corner of the dock and insert in the slot. Push the cartridge gently into the dock until it clicks in place.
- To unload a cartridge, push the eject button on the RDX dock or use the DataGuard Management Interface to select Device > External Drive > RDX-SATA > Remove.

When the cartridge has been ejected, pull the cartridge straight out (see Figure 2). If neither method works, you can insert a straightened paper clip into the Emergency Eject hole. This practice involves greater risk of data loss, so only use it if necessary. See the Troubleshooting section for further advice.

Write Protection

To prevent accidental erasure of an RDX cartridge, slide the write protection tab to the left (see Figure 3). To remove write protection, slide the tab to the right.

Caution
When using the emergency eject feature, apply force in a straight line only. Push until you feel resistance, then push once more to eject the cartridge. If the tool is angled while in use, damage may result.

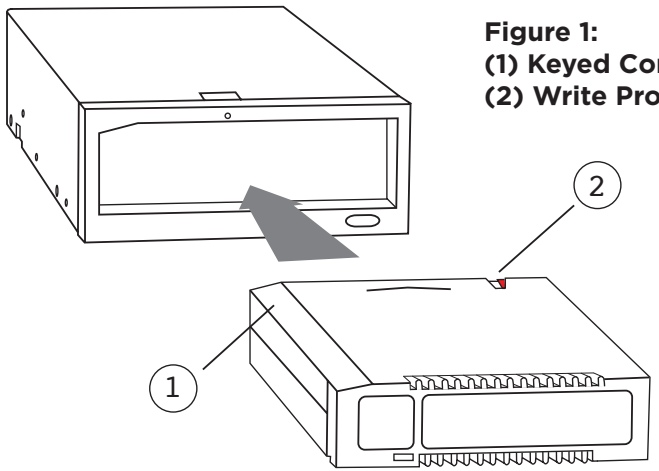


Figure 1:
(1) Keyed Corner
(2) Write Protect Tab

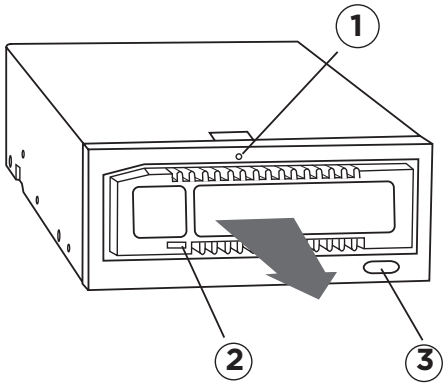


Figure 2:
(1) Emergency Eject hole
(2) Cartridge Indicator (on cartridge)
(3) Power Indicator/ Eject Button

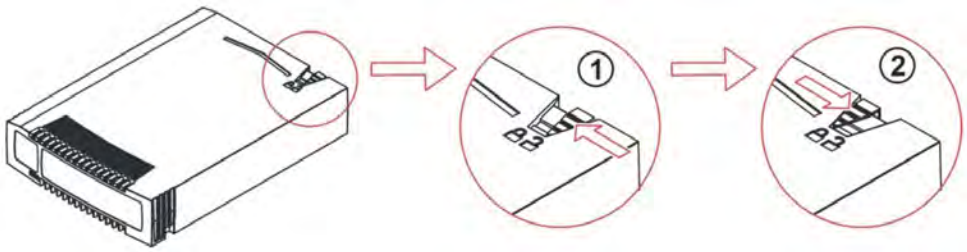


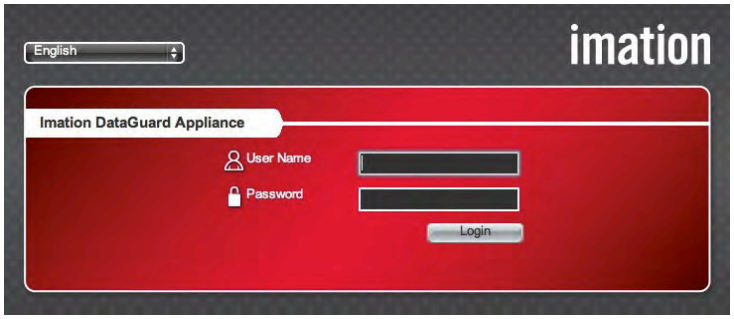
Figure 3:
(1) Cartridge unlocked (write protection off)
(2) Cartridge locked (write protection on)

DataGuard Management Interface

The DataGuard Management Interface works with most popular web browsers to let you manage the R4 or T5R. Once the device is powered on, is connected to the network and has an IP address, the DataGuard Management Interface can perform configuration and maintenance functions.

Using the DataGuard Management Interface

To use the DataGuard Management Interface, open a compatible web browser. Check the LCD display panel to find the IP address for the device. Type this address in the web browser and press Enter or Return. The browser should display a login screen.



Login Screen

1. Type the **User Name** in the field provided. The default user name is “administrator” and is case-sensitive.
2. Type the **Password** in the field provided. The default password is “password” and is case-sensitive.
3. Choose your **Language** preference from the drop-down list. The default language is English.
4. Click the **Login** button.
5. After a you log in successfully, the Dashboard will appear in the browser window. It displays System Status and other information about the DataGuard Appliance, and provides links to the most often used menus.

Note: Please change your password immediately after your login. From the **Administration** tab, click the **NAS User** menu item. Move your pointer over the **administrator** row, then click **Change Password**. Keep your administrator password in a safe place.

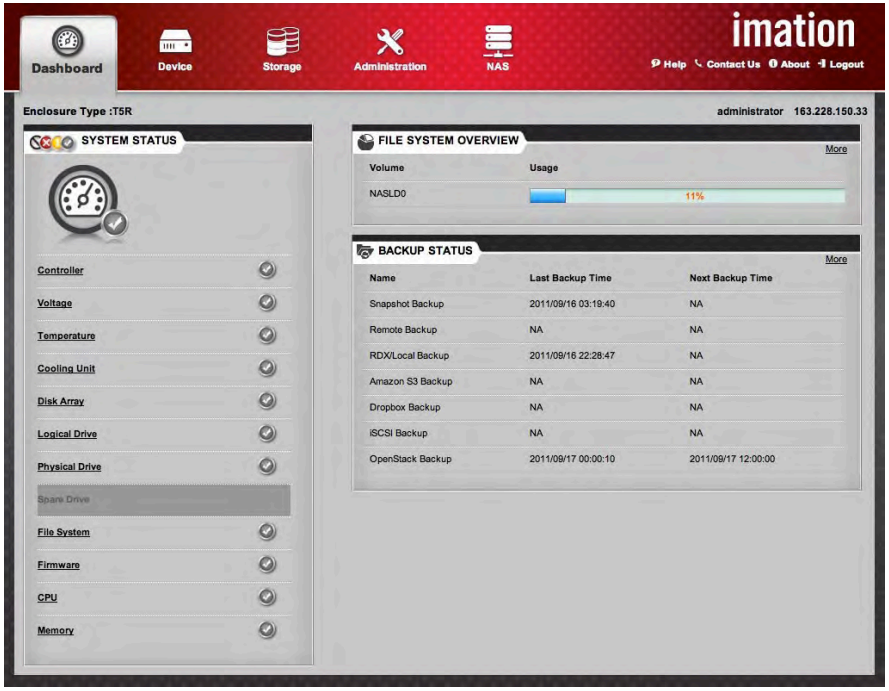
Dashboard Tab

The Dashboard tab displays top-level system status. When the system is functioning normally, a gray circle with a check mark will appear next to the speedometer icon. If errors are encountered, a red circle with an X will appear next to the speedometer icon. See the examples below.

The system is OK.

The system has detected errors.

If an error appears on a Dashboard item, click on the error symbol for details and instructions.



Dashboard

System Status

System Status alerts are linked to menus with configurable options and more information. Click any of the first five items listed—Controller, Voltage, Temperature, PSU (R4 only) or Cooling Unit—to view the Component List on the Device tab.

- Click Disk Array to view the embedded Create Disk Array menu on the Storage tab.
- Click Logical Drive to view the Logical Drive Management menu on the Storage tab.
- Click Physical Drive to view the Physical Drive menu on the Device tab.
- Click Spare Drive to view the Spare Drive Management menu on the Storage tab.
- Click File System to view the File System menu on the NAS menu tab.
- Click Firmware to view the Firmware updates menu on the Administration tab.

The conditions of various system functions are indicated by icons as follows:

The component is OK.

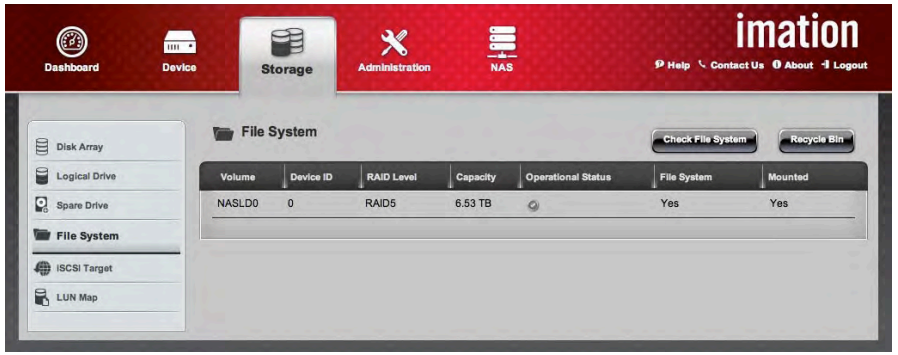
The component needs attention.

The component has failed.

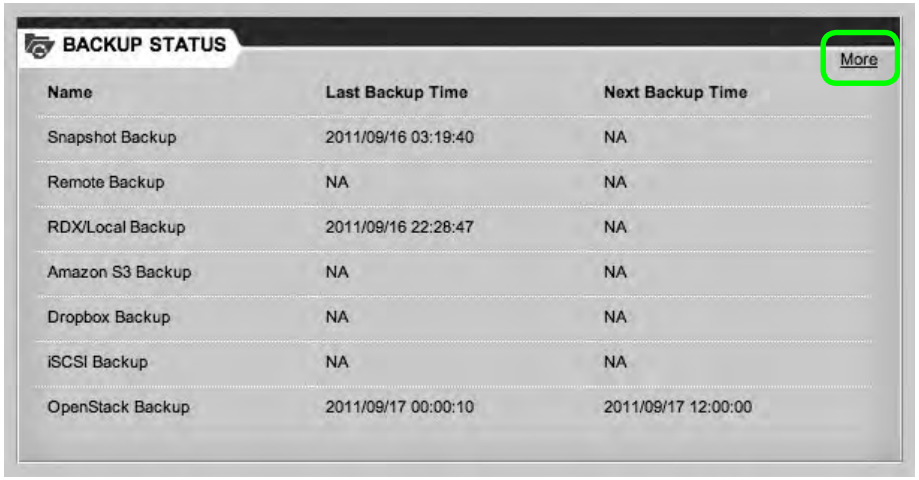
Dashboard > File System Overview

File System Overview

This area displays logical drives, their capacities, and the percentage of each in use. To view file system details or run diagnostic tests, click the “More” link at the top right. This will open the Storage tab and File System menu item, shown below.



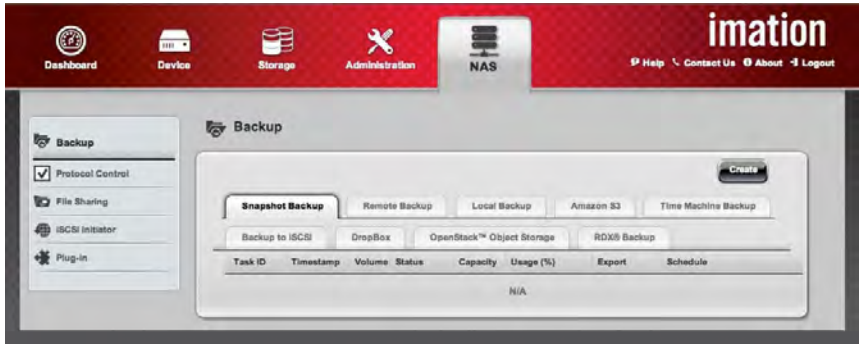
Storage > File System



Dashboard > Backup Status

Backup Status

This area displays the following backup types, plus the most recent and next scheduled backup times. To view the details of existing backups, or to create a new backup, click the “More” link at the top right. This will open the NAS tab and Backup menu item, as shown below.



NAS > Backup

Creating a New Backup

From this screen, you can select from multiple backup types:

- Snapshot Backup
- Remote Backup
- Local Backup
- Amazon S3
- Time Machine Backup
- Backup to iSCSI
- DropBox
- OpenStack™ Object Storage
- RDX® Backup

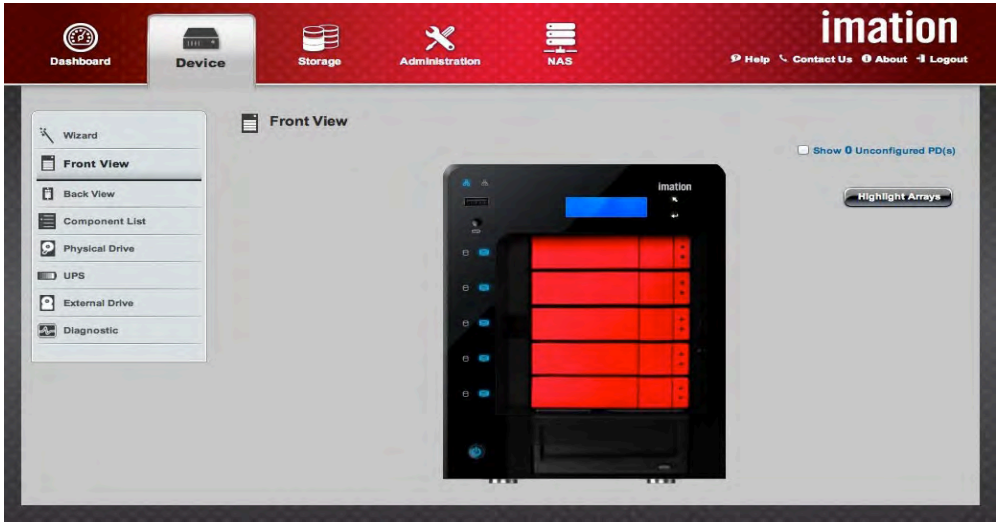
For detailed descriptions and instructions on each of these backup types, refer to the NAS Tab section beginning on page 62.

Device Tab

From this tab, you can review hardware configuration details for individual hard drives, system components and attached devices such as external storage or uninterruptible power supply units. The main panel of this tab shows the Front View of the DataGuard Appliance and includes a menu with the following items:

- Wizard—Helps you configure network and hard drive settings for the appliance
- Front View—Shows graphical information about the hard drive slots, indicators and controls
- Back View—Shows graphical information about interface and power connections
- Component List—Provides current condition of enclosure, controller, buzzer, LED and fan
- Physical Drive—Lists installed hard drives by ID, status, model, type, location, configuration and capacity
- UPS—Shows information about uninterruptible power supply (if present)
- External Drive—Lists external drives by ID, status, model, type, location, total capacity and cache
- Diagnostic—Tests hard drives, network ports, IP routing and DNS setting

Device > Front View (R4)



Device > Front View (T5R)

Setup Wizard

To use the Setup Wizard for configuring disk settings, log in to the DataGuard Management Interface and click at Device tab.

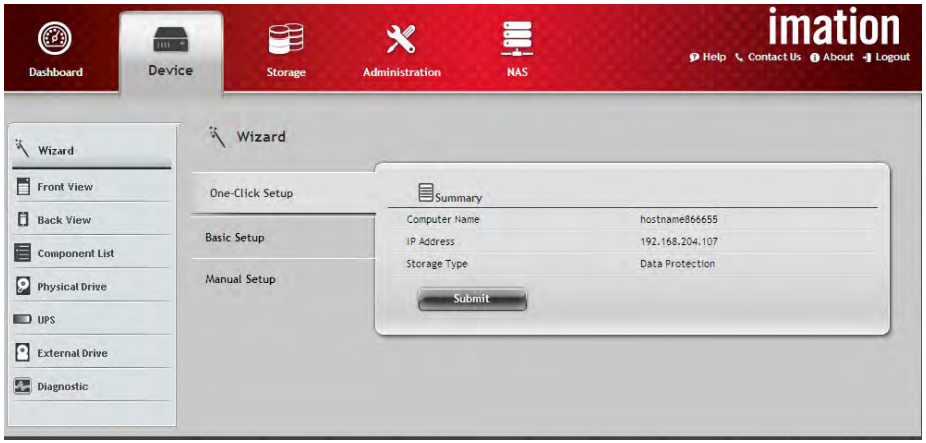
One-Click Setup

To use the **One-Click Setup** option, follow the instructions below. From the **Device** tab, click **Wizard** on the left menu. The Wizard will show three options: One-Click Setup, Basic Setup, and Manual Setup.

1. Click the **One-Click Setup** button. The application will automatically assign a **Computer Name, IP Address** and **Storage Type**.
2. Review these items in the **Summary** table. To change any setting, click the **Back** button to return to a previous menu. To accept the proposed configuration, click the **Submit** button.

Setup will continue automatically; disk configuration will take time. DataGuard Appliances with more or larger hard drives will take longer. Progress is displayed during the initialization process.

3. When the setup process is finished, the message **Setup Wizard Complete** will appear.



Device > Wizard > One-Click Setup

RAID Settings

The DataGuard Appliance uses RAID (redundant array of independent disks) technology to manage multiple hard drives as if they are one storage device. As more hard drives are added, higher levels of performance and redundancy become possible. If you use the One-Click Setup option, the DataGuard Management Interface selects the RAID type automatically based on the number of the hard drives installed:

Number of installed hard drives	1	2	3	4	5
RAID type	RAID0	RAID1	RAID5	RAID5	RAID5

If you plan to create multiple arrays or logical drives, or if you want to specify a particular RAID level, click the **Manual Setup** button and refer to “Storage Tab” on page 3017 for instructions.

Important

Once setup is complete, the DataGuard Appliance will synchronize its internal hard drives, a process that can take up to several hours. Although the device can be used during this time, disk activity will be higher and performance will be slower than usual.

Basic Setup

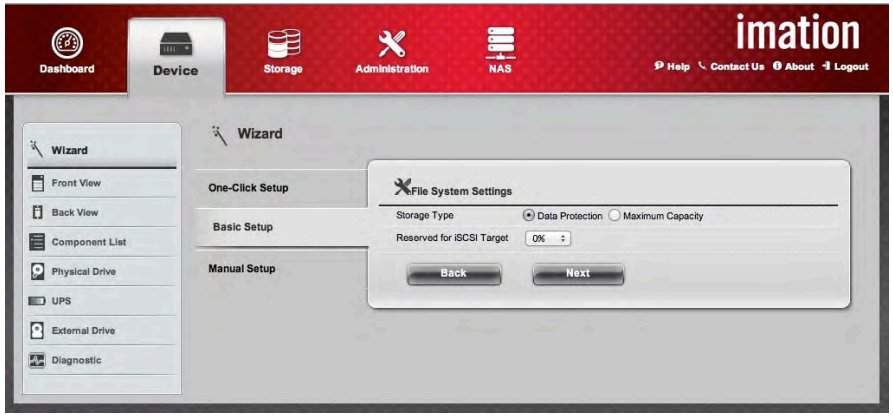
If you prefer to override the automatic RAID level configuration, or want to configure IP settings for the DataGuard Appliance, follow these instructions:

1. From the **Device** tab, click **Wizard** on the left menu, then click **Basic Setup**. The active screen will display network settings and device name configuration.
2. Enter a name in the Computer Name field. This name will appear on the network.
3. To get IP settings from an active DHCP server, select **Obtain an IP address automatically;** to assign a fixed IP address, select **Configure IP settings manually** and enter an IP address.

Device > Wizard > Basic Setup > Network Settings

Use the **File System Settings** menu to choose a RAID preference for *Data Protection* or for *Maximum Capacity*; and choose whether any or all of the drive capacity will be assigned for use as an iSCSI target:

1. Choose **Data Protection** for RAID level 1 or above (depending how many disks are installed).
2. Choose **Maximum Capacity** for RAID 0.
3. To create capacity for iSCSI target, use the **Reserve for iSCSI Target** pull-down menu to select a percentage of the total capacity to use for iSCSI.

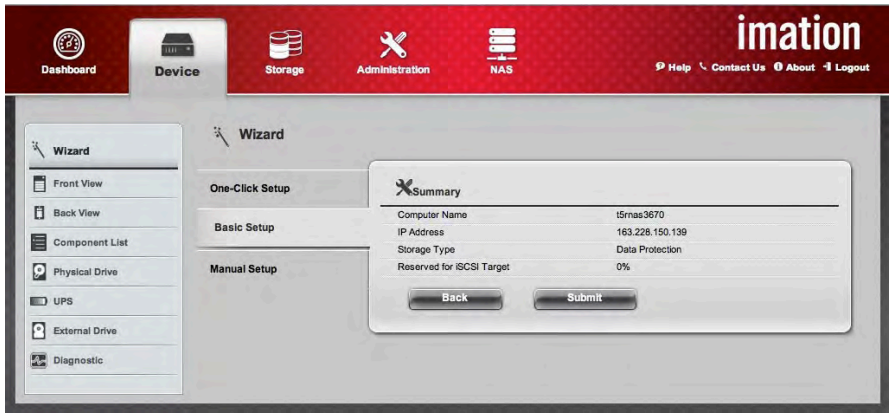


Device > Wizard > Basic Setup > File System Settings

The **Summary** window will display the **Computer Name, IP Address, Storage Type** and **Capacity** reserved for iSCSI Target (percentage of total, if selected in previous menu).

1. To change any setting, click the **Back** button to return to a previous menu. To accept the proposed configuration, click the **Submit** button.

Setup will continue automatically; disk configuration will take time. DataGuard Appliances with more or larger hard drives will take longer. Progress is displayed during the initialization process.

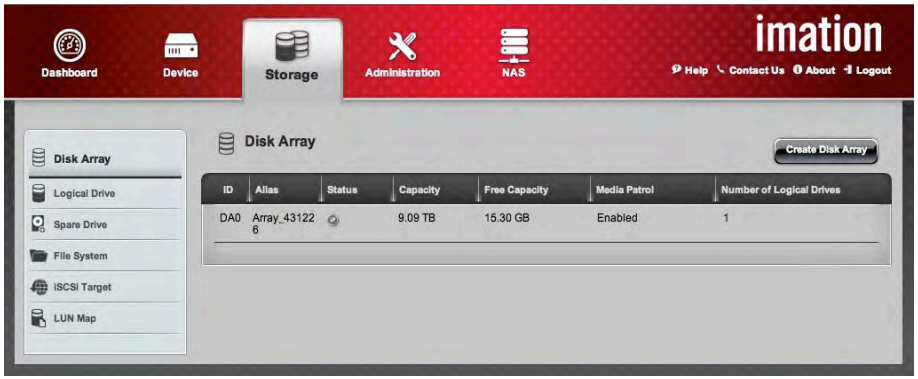


Device > Wizard > Basic Setup > Summary

Manual Setup

To use the **Manual Setup** option, follow the instructions below.

1. From the **Device** tab, click **Wizard** on the left menu, then click **Manual Setup**. The Storage tab will open to the Disk Array menu item.



Device > Wizard > Manual Setup

2. Click the **Create Disk Array** button at top right**.** The window will expand to show a front view of the DataGuard Appliance, with configuration options in text fields, menus and check boxes.

Device > Wizard > Manual Setup > Create Disk Array (R4)

Device > Wizard > Manual Setup > Create Disk Array (T5R)

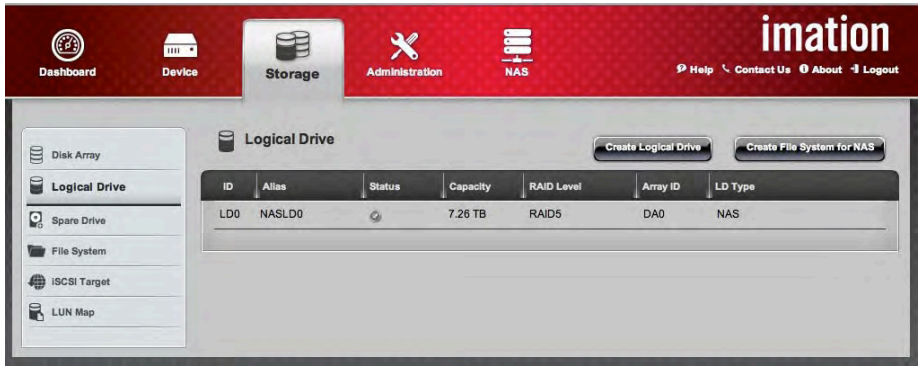
3. In the **Alias** field, enter up to 32 characters (including letters, numbers, space between characters, and underscores).
4. Select the check boxes for the features you want to enable:
   a. **Media Patrol** checks the magnetic media on all physical drives assigned to disk arrays, and on spare drives, as part of routine maintenance.
   b. **Predictive Data Migration (PDM)** automatically copies data from hard drives on which errors are detected to an assigned spare drive. Refer to page 37 for instructions on assigning a spare drive.
   c. **Power Management** allows hard drives to enter standby mode after they are idle for a set period.
5. Use the **Media Type** menu to select the type of drive or drives in the array. All drives in an array must be either hard disk drives or solid state drives. You cannot mix media types in a single array.
6. **Select Physical Drives** lets you click the drives on the image of the DataGuard Appliance to add them to your disk array. The ID numbers of the selected drives will appear in the field below the diagram.
7. Review these items in the **Summary** table. To change any setting, click the **Back** button to return to a previous menu. To accept the proposed configuration, click the **Submit** button.
8. When the setup process is finished, the message ***Setup Wizard Complete*** will appear.

- To create additional disk arrays, click the **Create More** button.
- If you are done creating disk arrays, click the **Finish** button.

Create Logical Drives

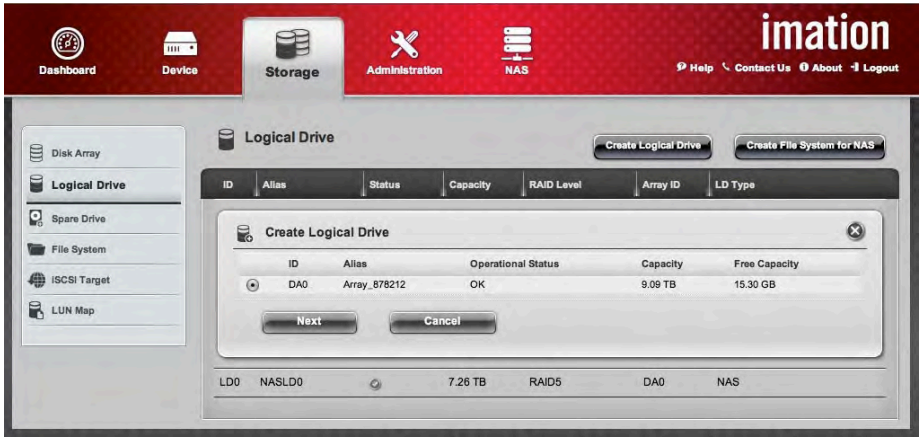
After creating a disk array, you need to create a logical drive on it, following the steps below.

1. Click the **Storage** tab, then the **Logical Drive** menu item to show this panel:



Storage > Logical Drive

2. Click the **Create Logical Drive** button to show this panel:



Storage > Logical Drive > Create Logical Drive

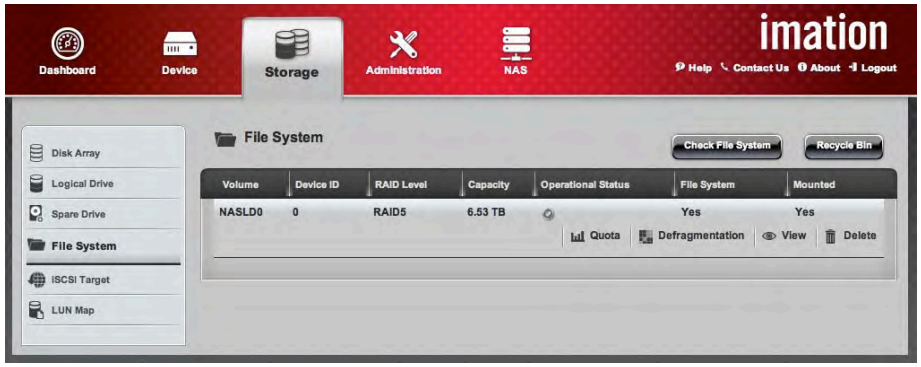
3. Select the disk array you want to use and click the **Next** button.

Storage > Logical Drive > Create Logical Drive > Settings

4. In the **Create Logical Drive** window, complete the required settings:
   a. In the **Alias** field, enter up to 32 characters (including letters, numbers, space between characters, and underscores).
   b. Set the **LDType** as NAS or iSCSI Target.
   c. Select a **RAID Level** from the drop-down menu; available options depend on the number of physical drives installed.
   d. In the **Capacity** field, accept the default maximum capacity or enter a lesser capacity in MB, GB or TB. Any remaining capacity is available for an additional logical drive.
   e. Choose the **Stripe** size: 64 KB, 128 KB, 256 KB, 512 KB, or 1 MB. (See “Stripe Size” on page 3333)
   f. Choose the **Sector** size: 512 B, 1 KB, 2 KB, or 4 KB. (See “Sector Size” on page 3333)
   g. Choose the **Read Policy:** Read Cache, Read Ahead, or No Cache (see “Stripe Size” on page 3333)
   h. Choose the **Write Policy:** Write Back or Write Through. (See “Write Policy” on page 3333)
   i. Click the **Add** button.
   j. The new logical drive appears in the **New Logical Drives** list. If there is capacity remaining, you can create an additional logical drive.
5. When done, click the **Submit** button. The new logical drive(s) will appear in the **Logical Drive** list. New logical drives are automatically synchronized. You can access the logical drive during synchronization.
6. For logical drives configured as a NAS logical disk (LDType NAS) it is now necessary to create a file system. See the next page for instructions to continue setting up the logical drive.

Create File System

After you create one or more logical drives on the NAS, you need to create a file system. Click the **Create File System for NAS** button to jump to the **File System** menu on the **Storage** tab. You can also click the **Storage** tab and then the **File System** menu. The following panel will appear:



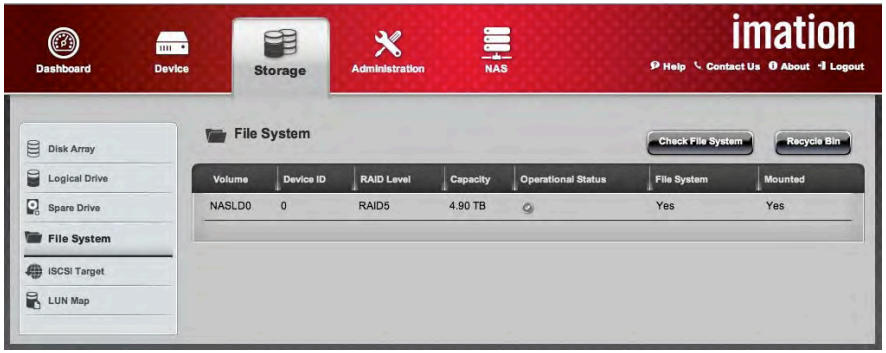
Storage > File System

This panel will display information about the Volume, Device ID, RAID Level, Capacity, Operational Status, File System, and whether the volume is Mounted. Click on the row below these headings to view these additional options:

- Quota—Sets restrictions on user and group capacity
- Defragmentation—Rearranges data into contiguous blocks; can be scheduled
- View—Shows Volume, RAID Level, Operational Status, Capacity, Free Capacity, Used Capacity, and Usage; also lets administrator assign capacity or expand file system (if capacity allows)
- Delete—Allows administrator to delete all data on the selected file system

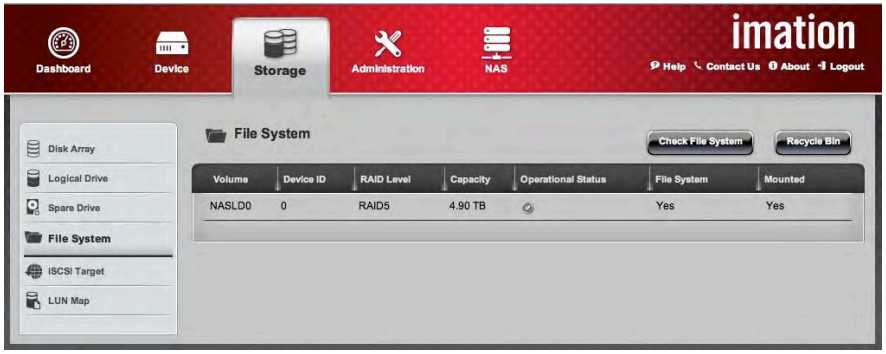
Note: iSCSI devices will not be shown on this screen.

Use the **Check File System** button to check the file system for errors and correct them automatically.



Storage > File System > Check File System

The **Recycle Bin** contains files that have been deleted by users or the administrator. When this feature is enabled, it appears as a shared folder. Click the Recycle Bin button to enable, disable, or empty it.



Storage > File System > Recycle Bin

Front View

Front View displays information about the DataGuard Appliance and any installed drives.

View Drive Information

- Move your pointer over the image of a drive carrier to see the device ID, physical capacity and operational status for that hard drive. Click on the carrier image for more detailed information.

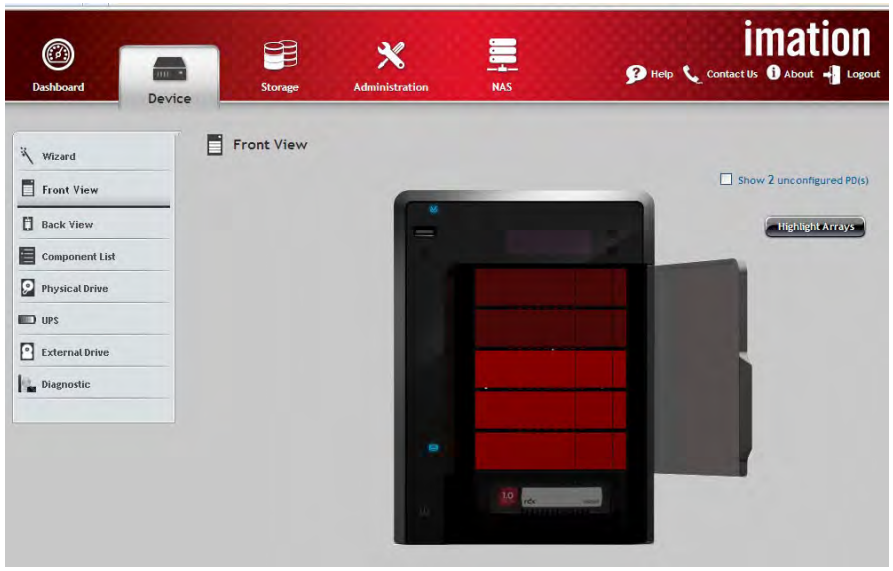
Show Unconfigured Physical Drives

- Click the **Show Unconfigured PD(s)** box to identify any unconfigured physical drives; these will appear in light green.

Highlight Disk Arrays

- Click the **Highlight Arrays** button to reveal a drop-down menu that shows existing disk arrays. Physical drives assigned to a disk array appear in purple.
  - ✓ Select All DA to show all disk arrays; all assigned hard drives will be highlighted.
  - ✓ Select DA0 (DA1, DA2, etc.) to show a specific disk array; only the hard drives assigned to that array will be highlighted.
  - ✓ Select close to close the menu and return to normal view.

Device > Front View (R4)



Device > Front View (T5R)

Device > Back View (R4)

Device > Back View (T5R)

Device > Back View > Internal (R4)

Device > Back View > Internal (T5R)

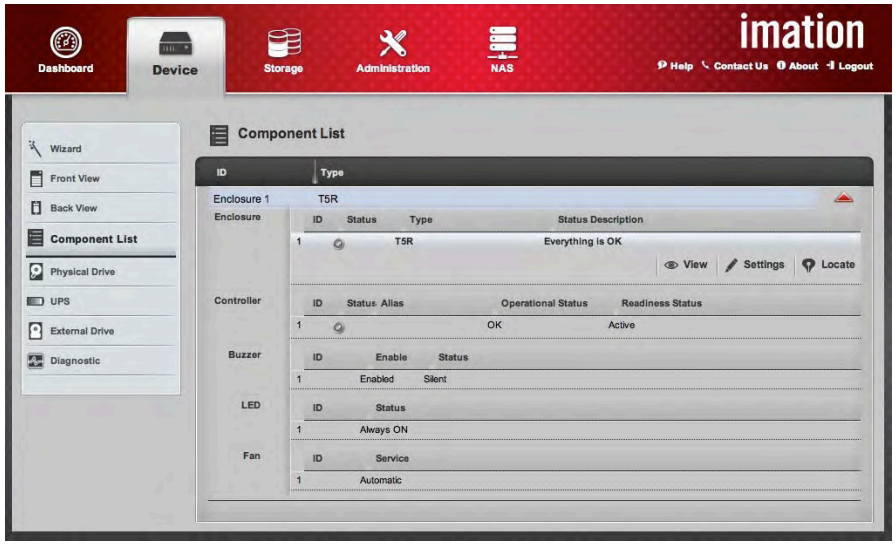
Back View

Select the **Back View** menu item to display the DataGuard Appliance back panel.

- Move your pointer over the power supply, Ethernet, USB, and eSATA network ports to see power supply status, connected device status, and network information.
- Click **Show Internal Components** to display a virtual view of the internal components. Move your pointer over these items to view CPU usage, controller board temperature, system temperature, memory usage, and enclosure information.

Component List

From the Device tab, select the **Component List** menu item to display the device ID, operational status, enclosure type, and status description of all enclosures. To view details, click the red triangle at right. A panel like the one below will appear.



Device > Component List > Overview

Move your pointer just below the ID for each item to view details and confirm or change settings. Here are the options for each component:

Enclosure

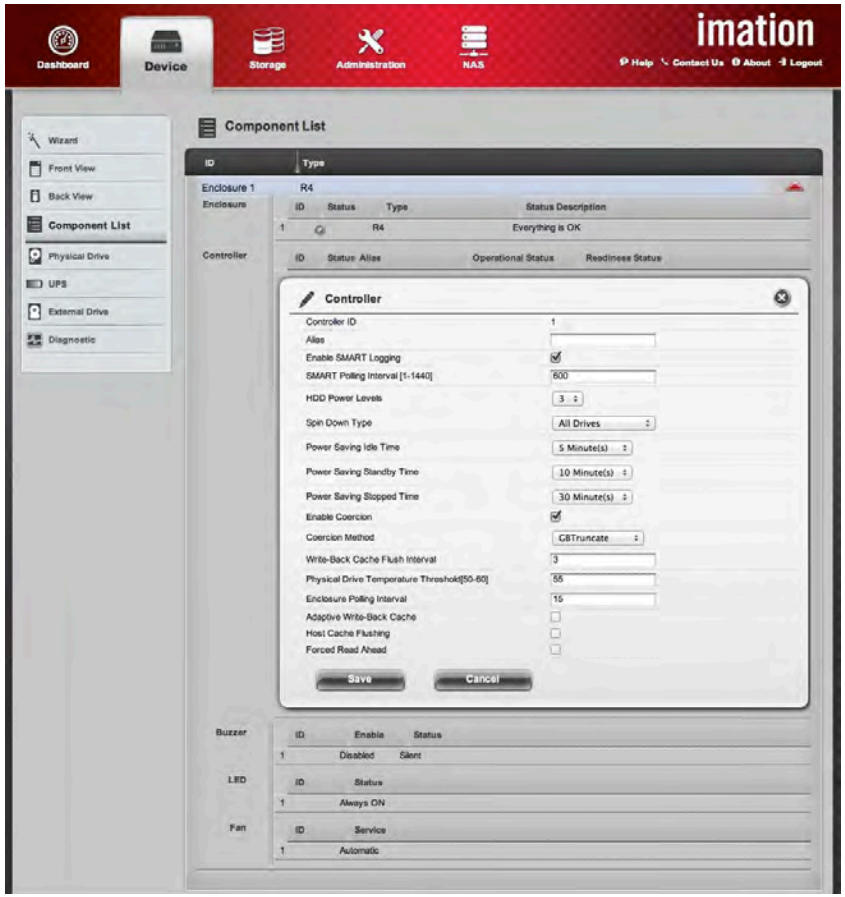
- **View**:
  - ✓ Click the View button to display enclosure ID and type; power supply unit ID and status; and information on the blower, temperature, and voltage
- **Settings**:
  - ✓ Click the Settings button to display warning temperature and critical temperature for the unit; you can also change these settings and confirm or cancel the changes
- **Locate**:
  - ✓ Click to activate; the enclosure will sound an audible alarm and the System Status LED will blink for one minute

Controller

The controller manages physical hard drives, representing them as logical drives as configured by the user. It also provides an additional memory cache for read/write operations of the RAID device. Use these menus to view or configure controller settings:

- **View**:
  - ✓ Move your pointer over the controller and click the View button to display the controller information list.
- **Settings**:
  - ✓ Move your pointer over the controller and click the Settings button.
  - ✓ Make setting changes as required (see below for details).
  - ✓ Click the Save button.

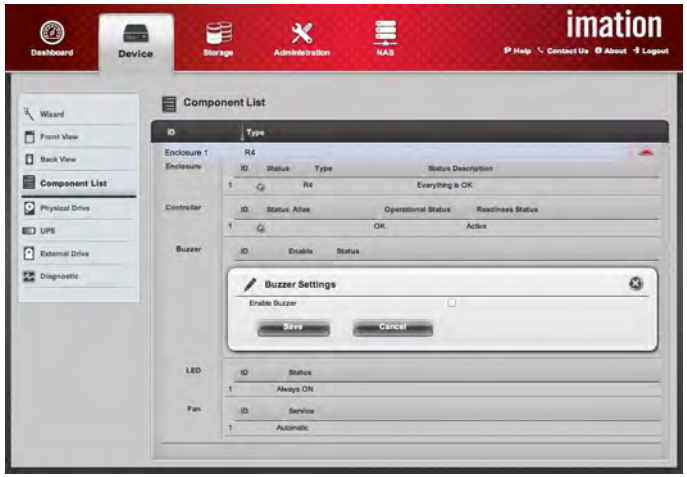
See the illustration and list on the next page to view the available parameters.



Device > Component List > Controller > Settings

Controller

- **View > Information:**
  - ✓ Controller ID
  - ✓ Readiness Status
  - ✓ Power On Time
  - ✓ Part Number
  - ✓ Cache Usage Percentage
  - ✓ Boot Loader Version
  - ✓ Firmware Version
  - ✓ Software Version
- **View > Advanced Information:**
  - ✓ Memory Type and Size
  - ✓ Controller Role
  - ✓ Flash Type and Size
  - ✓ NVRAM Type and Size
  - ✓ Preferred and Actual Cache Line Size
  - ✓ Coercion and Method
  - ✓ SMART Status and Polling Interval
  - ✓ Write-Back Cache Flush Interval
  - ✓ Physical Drive Temperature Threshold
  - ✓ Enclosure Polling Interval
  - ✓ Adaptive Write-Back Cache
  - ✓ Host Cache Flushing
  - ✓ Forced Read Ahead
  - ✓ HDD Power Levels
  - ✓ Spin Down Type
  - ✓ Power Saving Idle, Standby, and Stopped Time
- **View > Statistics:**
  - ✓ Data Transferred
  - ✓ Write Data Transferred
  - ✓ Non-Read/Write Errors
  - ✓ Write Errors
  - ✓ Non-Read/Write Request
  - ✓ Write IO Request
  - ✓ Statistics Collection Time
- **Settings:**
- Controller ID
  - ✓ Alias
  - ✓ Enable SMART Logging
  - ✓ SMART Polling Interval [1-1440]
  - ✓ HDD Power Levels
  - ✓ Spin Down Type
  - ✓ Power Saving Idle, Standby, and Stopped Time
  - ✓ Enable Coercion and Coercion Method
  - ✓ Write-Back Cache Flush Interval
  - ✓ Physical Drive Temperature Threshold[50-60]
  - ✓ Enclosure Polling Interval
  - ✓ Adaptive Write-Back Cache
  - ✓ Host Cache Flushing
  - ✓ Forced Read Ahead



Device > Component List > Buzzer > Settings

Buzzer

- Check the **Enable Buzzer** box to allow use of the buzzer, then click the **Save** button.
- Uncheck the **Enable Buzzer** box to silence the buzzer, then click the **Save** button.

Device > Component List > LED > Settings

LED

- Move your pointer over LED and click the **Settings** button to set LED options.
- Use the Daily option to schedule a time period each day to turn on LEDs.
- Use the pull-down menus to set a range of time to turn on LEDs by hour:minute to hour:minute.
- Click the **Save** button to apply and save these settings.

Device > Component List > Fan > Settings

Fan

- Choose the Automatic option (recommended) to run fans automatically in order to maintain the target HDD temperature. Set the target temperature with the Target Temperature (HDD) pull-down menu.
- Choose Manual to run the fan at a constant speed. Set the fan speed with the Fan Level pull-down menu.

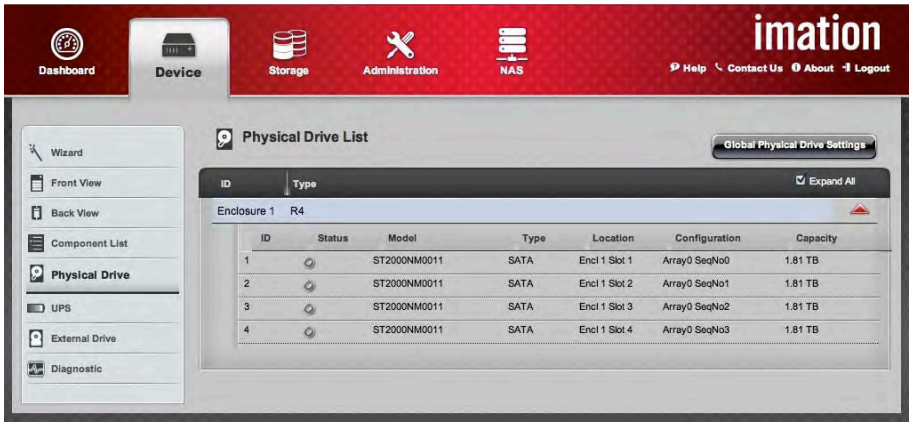
Warning

Fan speed settings are crucial for safety and system function. If you choose the manual setting, DO NOT set fan speed too low. Inadequate cooling can destroy hard disks and create a fire hazard.

Controller Setting	Description	Controller Setting	Description
Controller ID	ID of the controller for which settings are to be configured. The ID itself is not configurable.	**Alias**	Allows you to create a name for the DataGuard Appliance.
Enable SMART Log	Check the box to enable or uncheck to disable SMART Log.	**SMART Polling Interval**	Enter a value of 1 to 1440 minutes in this field to set SMART polling frequency.
HDD Power Levels	Choose the following options: • Level 0: Disabled • Level 1: Park R/W heads • Level 2: Slow down (must be supported on HDD) • Level 3: Spin down	**Spin Down Type**	Determines which hard drives spin down when idle: all hard drives or spare hard drives only.
Power Saving Idle Time	How long disks can be idle before putting them into standby mode.	**Power Saving Standby Time**	How long disks can be in standby mode before they are put in stopped mode.
Power Saving Stopped Time	How long disks can be in stopped mode before shutting down the system.		
Enable Coercion for fault-tolerant logical drives (RAID 1, 5, 6).	If possible, use hard drives of the same size, speed, make and model in your disk arrays. Hard drives of different sizes will work but the system must reduce or coerce the capacity of the larger drives to match the smaller ones. Capacity Coercion also allows you to use a replacement drive that is up to 1GB smaller than the working drive it backs up. For example, a working drive can be 80.5GB and the replacement drive can be 80.3, since all are rounded down to 80GB. Without Capacity Coercion, the controller will not permit the use of a replacement drive that is slightly smaller than the remaining working drives.	**Coercion Method**	Choose a method from the drop-down menu: • GB Truncate (default)—Reduces the useful capacity to the nearest 1,000,000,000 byte boundary. • 10GB Truncate—Reduces the useful capacity to the nearest 10,000,000,000 byte boundary. • Group Rounding—Uses an algorithm to determine how much to truncate; results in the maximum amount of usable drive capacity. • Table Rounding—Applies a predefined table to determine how much to truncate.
Write Back Cache Flush Interval	An interval for periodic controller flushes of the write cache to logical drive storage. This safety measure prevents the accumulation of data in cache that could be lost in the event of power loss.Enter a value of 1 to 12 seconds in this field; be aware that shorter intervals might affect applications in which read/write performance is crucial.	**Phydrv Driver Temperature Threshold**	Enter a temperature threshold value from 50 to 60 degrees Celsius. This is a temperature tolerance level that applies to the temperature of the physical drives.
Enclosure Polling Interval	The interval at which the array controller polls the environmental services processor in the enclosure. Default value is 15 ms; valid values are 15–255 ms.	**Adaptive Writeback Cache**	Adaptive Writeback Cache: • UPS power good: write back • UPS power fail: write through • No UPS: write through
Host Cache Flushing	Used to optimize data reliability, but can cause dropped frames when using high bandwidth, low latency tolerant or real-time applications. Disable this feature if the DataGuard Appliance is used as file storage for video editors or video capture software. To reduce the risk of data loss with host cache flushing disabled, connect the DataGuard Appliance to an uninterruptible power supply (UPS).	**Forced Read Ahead**	Can improve performance for multiple stream backup and sequential I/O. Use with logical drive read ahead enabled.

Physical Drive

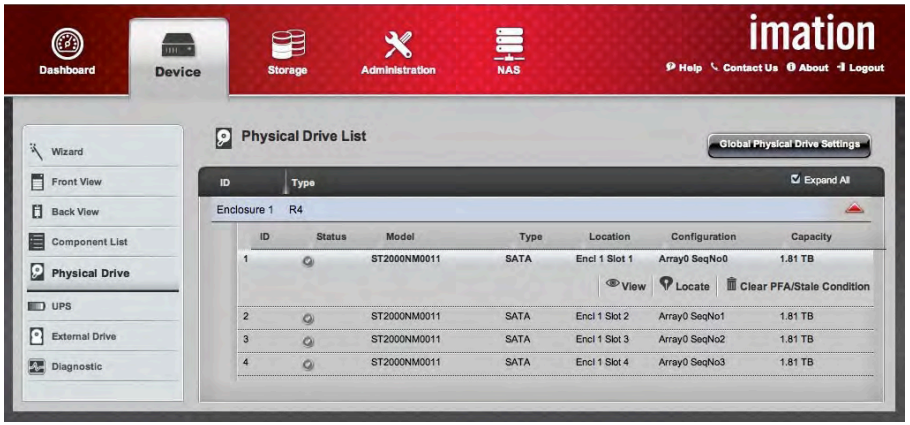
From the Device tab, click the **Physical Drive** menu item to display a list of physical drives.



Device > Physical Drive List

Physical Drive Information	Description
ID	Shows the identifier number of the physical drive
Status	Gray, yellow, and red icons (see examples at right)
Model	Displays the make and model of the drive
Type	Serial Advanced Technology Attachment (SATA)
Location	Shows enclosure number and slot number
Configuration	Lists the array number and sequence number for configured drives; other possibilities are Spare Number, Unconfigured, or Stale Configuration
Capacity	Shows the total storage capacity of physical drive

To view more detailed information for an individual drive, move your pointer over the physical drive and click the **View** button.



Device > Physical Drive List > View

Physical Drive Status Icons

The physical drive is OK.

The physical drive needs attention.

The physical drive has failed.

Physical Drive Problems

A physical drive problem can affect the entire DataGuard Appliance. When a yellow icon or a red icon appears for the status of a physical drive, check the operational of the hard drive:

1. Move your pointer over the physical drive and click the **View** button.
2. Check the Operational Status item.

Locate a Physical Drive

From the **Physical Drive** panel, move your pointer over the listed physical drive and click **Locate**. The drive status LED on the front panel will blink for one minute.

Global Physical Drive Settings	Description
Enable Write Cache	Helps optimize performance for multiple stream backup, restoration and elimination of redundant data (deduplication). Differs from controller-level cache because physical drive write caches are not protected. If power is lost or a drive is physically removed from the array during operation, unwritten data in the physical drive write caches will be lost. Write caching is beneficial for write intensive applications such as video editing that use large amounts of temporary files or tend to write in bursts. However, applications that continuously write large amounts of data will fill up the cache, which can slow down throughput. Enabled by default.
Enable Read Look Ahead Cache	Can improve I/O performance for applications that typically read data sequentially or on sequential sectors. Enabled by default.
Enable Command Queuing	Allows hard disks to optimize the order in which read/write commands are executed. This minimizes head movement to reduce physical drive wear, and can improve performance. Enabled by default.
DMA Mode	Lets you choose the mode used for Direct Memory Access controller of the physical disk.
Medium Error Threshold	The number of bad blocks tolerated before the controller marks a physical drive as Dead. By enabling this setting, you can identify problem drives before they fail, improving system performance and reliability. The default setting is 0 (disabled).
Automatic Acoustic Management	A method for reducing hard drive noise. This feature will function only if the installed disk drives support AAM. Enabled by default.
Automatic Acoustic Level	Determines whether drives will put more emphasis on noise reduction or performance. The default setting is low noise.

Device > Physical Drive > Global Physical Drive Settings

Uninterruptible Power Supply (UPS)

Every DataGuard Appliance allows the use of an uninterruptible power supply (UPS) that supports the APC UPS protocol. The UPS can connected by USB or Ethernet. Follow these steps to configure UPS features:

1. From the **Device** tab, click the **UPS** menu item.
2. Click the **Setup** button at the upper right.
3. Select your preferred settings for Interface, Power Off Threshold, and IP Address.
4. To confirm and apply your selections, click **Submit.** To return to the current settings, click **Cancel.**

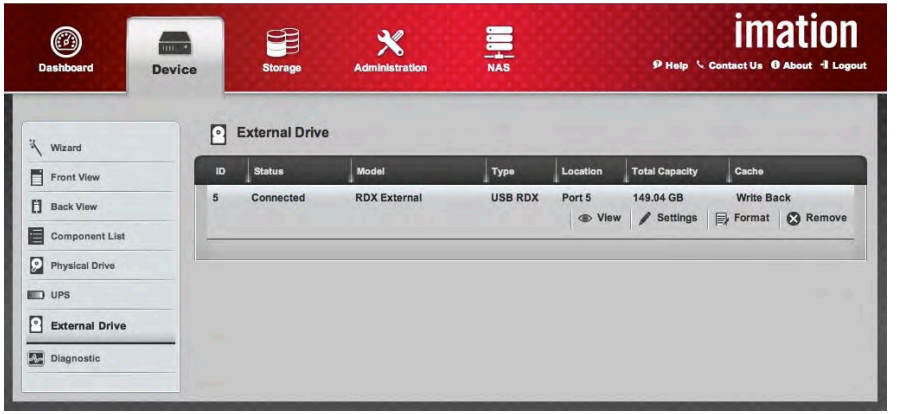
Device > UPS > Setup

UPS Settings	Description
Interface	Choose the type of UPS connected to the device, USB or Network.
Power Off Threshold	Select the Power Off Threshold option: Disabled, Immediate, The reserve power reaches [choose percentage] or After running [choose time to run].
IP Address	For Network UPS systems, enter the applicable IP address.

External Drive

External hard drives can be attached to the DataGuard Appliance through any of the five USB ports, and configured through the External Drive menu in the Management Interface. A drive that has already been formatted will connect automatically when powered on and connected. If a drive has not been formatted, it must first be formatted through the Format menu before it can be mounted.

Note: Refer to pages 3–6 for USB port locations on the DataGuard R4 and T5R.

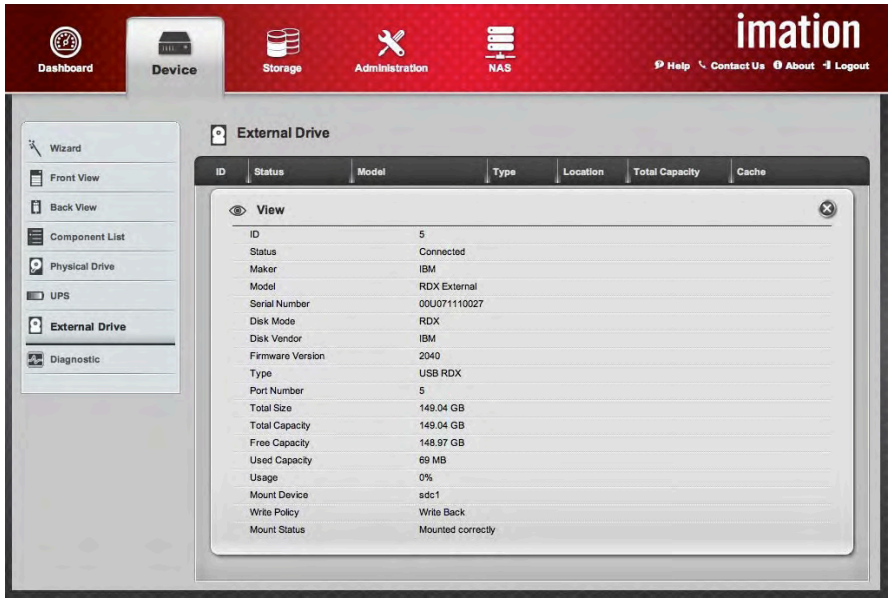


Device > External Drive

Managing an External Drive

1. From the **Device** tab, click the External Drive menu item.
2. Move your pointer over the external drive on the list to select one of the following options:

- Click **View** to display information about the drive.
- Click **Settings** to set the Write Policy (*Write Through* or *Write Back*), then click **Submit** to apply the new setting, or click **Cancel** to keep the current setting.
- Click **Format** to specify format type (FAT32, NTFS, or XFS for hard drives or flash drives, NTFS only for RDX cartridges); click **Submit** to format and mount the external drive, or click **Cancel** to keep the current setting.
- Click **Remove** to unmount the external drive, then click **Confirm** to apply your selection, or click Cancel to leave the drive mounted.



Device > External Drive > View

Warning
To reduce the risk of data loss, click Remove before disconnecting a USB drive.

Diagnostic

Use the Diagnostic menu to run basic function diagnostics for the following items:

- Physical Drives (SMART)
- Network Port 1
- Network Port 2
- IP Routing
- DNS Setting

The results are presented as a simple Pass or Fail for each test. To run the basic tests, select the **Diagnostic** menu item, then click the **Check** button. The panel will display results similar to the image below.

Device > Diagnostic > Results

Storage Tab

The simplest way to configure installed disk drives is to use the Setup Wizard from the Device tab and select One-Click Setup or Basic Setup. For other configurations, begin with the Storage tab. From there, you can create, manage, and delete disk arrays, logical drives, and spare drives.

Before configuration, determine how the DataGuard Appliance will be used, then consider your options for disk arrays, logical drives, spare drives, RAID levels and file systems. If you plan to use iSCSI functions, determine the capacity of the iSCSI drive or drives before creating any logical drives.

Storage > Overview

Storage Overview

The first item on the Storage tab is a Disk Array overview, which provides the following information:

- ID—The identity number of the array, such as DA0, DA1, DA2, etc.
- Alias—A name for the array as it appears in the DataGuard Management Interface.
- Status—Shows operational status as a gray icon (OK), yellow icon (error) or red icon (failure).
- Capacity—Indicates the total data capacity of the disk array.
- Free Capacity—Displays unconfigured or unused capacity on the physical drives.
- Media Patrol—Shows whether the feature is enabled or disabled for this disk array.
- Number of Logical Drives—How many logical drives this disk array contains.

Configuration

To prepare a DataGuard Appliance for use, you will need to complete three major processes:

1. Create a disk array
2. Create a logical drive
3. Create a file system

Each of these processes will include multiple configuration options; read each section thoroughly before you apply new settings.

Warning

When you initialize a logical drive, all the data on the physical drives will be erased. Back up any important data before you initialize a logical drive.

Disk Array

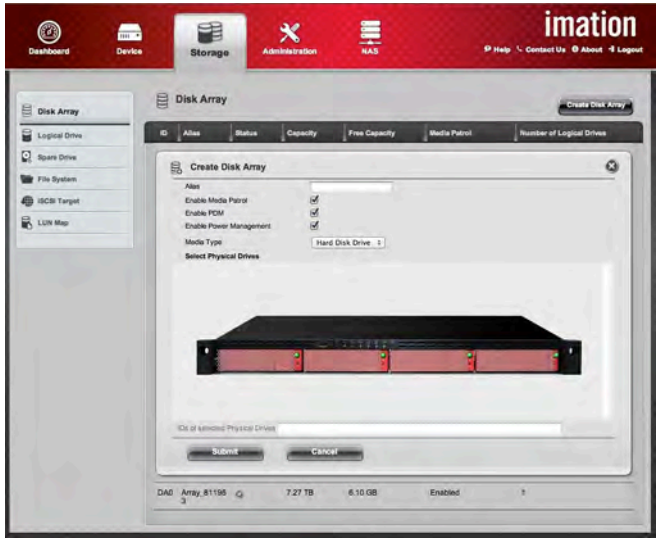
Create a Disk Array

From the Storage tab, click the Disk Array menu item. Then click the Create Disk Array button at the upper right of the panel. You can now enter the settings for a new disk array.

1. In the **Alias** field, enter up to 32 characters (including letters, numbers, space between characters, and underscores).
2. Select the check boxes for the features you want to enable:
   a. **Media Patrol** checks the magnetic media on all physical drives assigned to disk arrays, and on spare drives, as part of routine maintenance.
   b. **Predictive Data Migration (PDM)** automatically copies data from hard drives on which errors are detected to an assigned spare drive. Refer to page 37 for instructions on assigning a spare drive.
   c. **Power Management** allows hard drives to enter standby mode after they are idle for a set period.
3. Use the **Media Type** menu to select the type of drive or drives in the array. All drives in an array must be either hard disk drives or solid state drives. You cannot mix media types in a single array.
4. **Select Physical Drives** lets you click the drives on the image of the DataGuard Appliance to add them to your disk array. The ID numbers of the selected drives will appear in the field below the diagram.
5. Review these items in the **Summary** table. To change any setting, click the **Back** button to return to a previous menu. To accept the proposed configuration, click the **Submit** button.
6. When the setup process is finished, the message ***Setup Wizard Complete*** will appear.

- To create additional disk arrays, click the **Create More** button.
- If you are done creating disk arrays, click the **Finish** button.

Warning
Back up all important data before deleting a disk array, logical drive, or file system.



Storage > Disk Array > Create Disk Array (R4)

Storage > Disk Array > Create Disk Array (T5R)

Manage Disk Arrays

You can also use the Management Interface to change the configuration of an existing disk array:

1. From the Storage tab, click the Disk Array menu item. A list of disk arrays will appear on the panel.
2. Move your pointer over a disk array to show the available options: View, Settings, Locate, and Delete.

- Click View to display information about a disk array, or click Settings to change its configuration. The table below explains the meaning of each item in the information panel.
- Click Locate to identify physical drives. This feature will make the status LEDs blink for one minute on all physical drives used in the disk array.
- Click Delete to remove an array. If you choose this option it will be necessary to confirm the deletion in a new dialog. Click Confirm to delete the array or Cancel to keep it.

Note: If logical drives and a file system have been set up, it may be necessary to delete the file system and logical drive before the disk array can be removed.

Disk Array Information	Description
Disk Array ID	Disk array identifier: DA0, DA1, DA2, etc.
Alias	This is the alias assigned through the Disk Array Settings menu.
Operational Status	Displays the current state of the disk array.
Media Patrol	Indicates whether Media Patrol is enabled or disabled.
PDM	Indicates whether Predictive Data Migration is enabled or disabled.
Power Management	Indicates whether power management is enabled or disabled.
Total Capacity	Displays the total storage capacity of the disk array.
Configurable Capacity	Displays the total usable capacity of the disk array.
Free Capacity	Displays the unallocated capacity of the disk array.
Max Contiguous Free Space	Displays the unused capacity of the disk array in contiguous sectors.
Number of Physical Drives	The number of physical drives in the disk array.
Number of Logical Drives	The number of logical drives in the disk array.

Storage > Disk Array

Disk Array Problems

Problems typically result from a physical drive failure, such as a degraded or offline disk array. The RAID controller can rebuild a disk array that has become degraded. A more serious but less common problem is an incomplete array, which results from a physical drive that fails or goes offline during RAID level migration or disk array transport.

Disk Array Degraded

Disk arrays are made up of physical drives; logical drives are created on disk arrays. When a physical drive in a disk array fails, three things happen:

- The operational status of the disk array becomes Degraded.
- The operational status of the logical drive becomes Critical.
- The operational status of the physical drive becomes Dead or Offline.

Disk Array Offline

When a disk array and its logical drives go offline, data stored in the logical drives becomes inaccessible. Logical drives based on fault-tolerant disk arrays (RAID 1, 5, 6, or 10) go offline when two physical drives are removed or fail. Logical drives based on non-fault tolerant disk arrays (RAID 0) go offline when one physical drive is removed or fails.

RAID Levels

RAID arrays distribute data over multiple hard drives. RAID levels offer different ways of managing the way data will be written to and read from those hard drives. Some configurations are optimized for speed, others for redundancy. To choose the best RAID level for your purposes, begin by checking the standard practices for your field, and adjust to fit your specific requirements. For detailed descriptions of common RAID levels supported by the DataGuard Appliance, review the table on the next page.

Within each RAID level, you can configure stripe size and sector size. Although most users do not need to change these settings, here is a brief explanation of their role in balancing performance and redundancy The RAID levels supported will depend on the number of hard drives in the DataGuard Appliance. The table below shows the available RAID levels for the number of hard drives installed.

Level	Number of installed disks				
	1	2	3	4	5
RAID 0	X	X	X	X	X
RAID 1		X			
RAID 10				X	
RAID 1E		X	X	X	X
RAID 3			X	X	X
RAID 5			X	X	X
RAID 6				X	X

Stripe Size

As files are accessed, they are broken up and written to the logical drive in pieces called stripes. Because logical drives are made up of one or more physical drives, a stripe must be divided again. This subdivided part is called the stripe size. Put another way, a stripe size is the equal piece written to each physical drive in a disk array; each and stripe size is part of a stripe.

- When data is passed to the RAID controller, it is divided by increments of the stripe size to create one or more blocks. These blocks are then distributed among drives in the array, leaving different stripe-sized pieces on different drives.
- Increasing the stripe size reduces the number of drives that a given data file uses to hold all the blocks containing file data, while decreasing the stripe size increases that number.
- In theory, by increasing the number of drives used will improve transfer performance but diminish positioning performance. Increasing stripe size requires fewer drives, and, in theory, reduces transfer performance but improves positioning.
- Optimal stripe size depends on the user's performance requirements and what applications are running. Check the user documentation for the software you will be using, and for the hard drives in the array.

Sector Size

A sector is the smallest storage unit used on a hard drive. A primary consideration for determining what sector size to use is whether the logical drive will be configured for NAS or as an iSCSI Target (LDType setting). For iSCSI Target setups, the sector size should be optimized for the file system with which it will be used. Consult the user documentation of the system where it will be mounted and formatted.

Read Policy

The read policies determine if the controller reads sequential sectors of the logical drive. Options are:

- *ReadAhead*: The controller reads sequential sectors of the logical drive. Read-ahead policy can improve system performance if the data is written to sequential sectors.
- *ReadCache*: The controller reads cache information to determine if the data is available in the cache before retrieving the data from the disk. This can provide faster read performance.
- *NoCache*: The controller retrieves data directly from the disk and not from the cache.

Write Policy

Write policies determine if the controller sends a write-request completion signal once the data is in the cache or until after it has been written to disk.

- *WriteBack*: The controller sends a write-request completion signal as soon as the data is in the controller cache but has not yet been written to disk. Write-back caching might improve performance but also entails a data security risk since a system failure could prevent the data from being written to disk and data might be lost. Other applications can also experience problems when it is assumed that the requested data is available on the disk.
- *WriteThru*: The controller sends a write-request completion signal only after the data is written to the disk. Write-through caching provides better data security than write-back caching but lower performance.

Rebuilding a Logical Drive

When a physical drive within a logical drive is identified as Dead and the logical drive is identified as Critical, performing a rebuilding is necessary:

- For a fault tolerant RAID levels, (e.g. Raid 1, 5, 6, 10) if a spare drive is available, the logical drive will begin rebuilding automatically.
- For a fault tolerant RAID levels, if no spare drive is available, you must replace the failed hard drive. The logical drive will begin rebuilding automatically, when you install the new hard drive.
- RAID 0 logical drives go offline after a physical drive failure. A RAID 0 logical drive cannot be rebuilt. All data on the logical drive is lost.

Notes: Rebuilding can take several hours depending on the size of your physical drives. During a rebuild, you can access your folders on the DataGuard Appliance.

RAID Level	Description	Performance
RAID 0 Stripe	Data is split evenly across multiple disks, striping with no parity, no mirroring, no error checking and no redundancy. A disk failure will destroy the array and the probability of failure increases with the number of disk added to the array. Data blocks are written to their respective disks simultaneously on the same sector. This allows smaller sections of the entire chunk of data to be read off the drive in parallel, increasing bandwidth. More disks in the array provides higher data transfer rates, but with a greater risk of data loss. Storage space added to the array by each disk is limited to the size of the smallest disk, so the installed disks should be the same size. Stripe size is normally a multiple of the hard disk sector size (default 64KB/512 bytes). Useful for non-critical data that changes infrequently and is frequently backed up where redundancy is unnecessary or irrelevant and when excellent read/write performance is desirable such as audio or video streaming or editing applications.	Random Read Performance: Very good Random Write Performance: Very good Sequential Read Performance: Excellent Sequential Write Performance: Very good
RAID 1 Mirror	Creates an exact copy (mirroring without parity or striping) of a set of data on two or more disks. Used when reliability is more important than storage capacity. Can only be as big as the smallest member disk and can only use an even number of disks. One disk can remain inactive, as a backup and be used to rebuild the mirrored disk.	Random Read Performance: Good Random Write Performance: Good Sequential Read Performance: Fair Sequential Write Performance: Good
RAID 1E Enhanced Mirror	RAID 1E offers the security of mirrored data provided by RAID 1 plus the added capacity of more than two physical drives. It also offers overall increased read/write performance plus the flexibility of using an odd number of physical drives. With RAID 1E, each data stripe is mirrored onto two physical drives. If one drive fails or has errors, the other drives continue to function, providing fault tolerance. The advantage of RAID 1E is the ability to use an odd number of physical drives, unlike RAID 1 and RAID 10. You can also create a RAID 1E Logical Drive with an even number of physical drives. However, with an even number of drives, you obtain somewhat greater security with comparable performance using RAID 10. RAID 1E logical drives consist of three or more physical drives. You can create an array with just two physical drives and specify RAID 1E. But the resulting logical drive is actually a RAID 1.	Random Read Performance: Very good Random Write Performance: Very good Sequential Read Performance: Very good Sequential Write Performance: Very good
RAID 3 Block Stripe and Dedicated Parity	Uses byte-level striping across multiple disks with a dedicated parity disk. Parity information is sent to a dedicated parity disk, the failure of any disk (including the parity disk) in the array can be tolerated. The dedicated parity is a performance bottleneck for random writes especially, because it must be accessed any time data is written to the array. Performance problems might occur if it is necessary to service multiple requests simultaneously. I/O operation requires activity on every disk and synchronized spindles.	Random Read Performance: Fair Random Write Performance: Poor Sequential Read Performance: Very good. Sequential Write Performance: Fair to good
RAID 5 Block and Parity Stripe	Uses block-level striping with parity data distributed across three or more drives; requires all drives but one to be present to operate. The array is not destroyed if a single drive fails. If a drive fails, any subsequent reads are calculated from the distributed parity and the drive failure is unnoticeable to the end user. A single drive failure reduces performance of the entire array until the failed drive has been replaced and the associated data rebuilt.	Random Read Performance: Excellent Random Write Performance: Fair Sequential Read Performance: Good to very good Sequential Write Performance: Fair
RAID 6 Block and Double Parity Stripe	Extends RAID 5 by adding an additional parity block. It uses block-level striping with double distributed parity distributed across all member disks. Provides fault tolerance of two drive failures; the array continues to operate with up to two failed drives. Makes large RAID groups more practical, especially for high-availability systems. This is important because large-capacity drives lengthen the time required for recovery from the failure of a single drive. In the event of a single drive failure, single-parity RAID levels are as vulnerable to data loss as a RAID 0 array until the failed drive is replaced and its data rebuilt; the amount of time the rebuild takes increases with the size of the drive. Double parity gives time to rebuild the array without the data being at risk if a single additional drive fails before the rebuild is complete.	Random Read Performance: Very good to excellent Random Write Performance: Poor Sequential Read Performance: Good to very good Sequential Write Performance: Fair
RAID 10 Mirror / Stripe	Mirror + Stripe combines both of the RAID 1 and RAID 0 logical drive types. RAID 10 can increase performance by reading and writing data in parallel or striping, while protecting data by duplicating it or mirroring. The Imation DataGuard Appliance implements RAID 10 by creating a data stripe over one pair of disk drives, then mirroring the stripe over a second pair of disk drives. Some applications refer to this method as RAID 0+1. The data capacity RAID 10 logical drive equals the capacity of the smallest physical drive times the number of physical drives, divided by two. In some cases, RAID 10 offers double fault tolerance, depending on which physical drives fail. RAID 10 arrays require an even number of physical drives and a minimum of four. For RAID 10 characteristics using an odd number of physical drives, choose RAID 1E.	Random Read Performance: Very good Random Write Performance: Very good Sequential Read Performance: Very good Sequential Write Performance: Very good

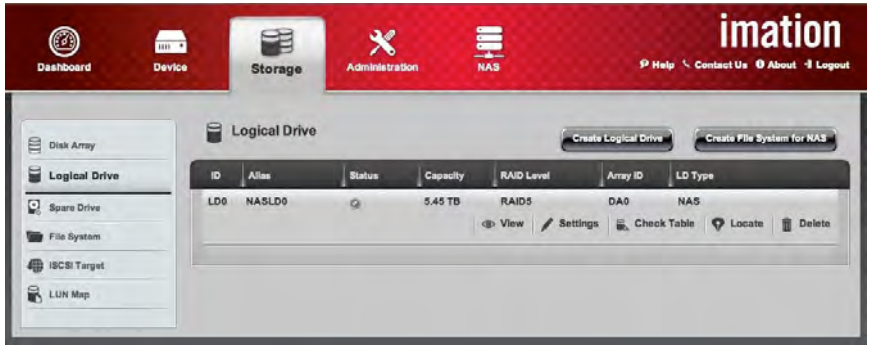
Logical Drive

Create Logical Drive

After creating a disk array, you need to create a logical drive on it. The logical drive can use part or all of the available storage capacity in the disk array. If the DataGuard Appliance will be used as data storage on an iSCSI SAN, you will need to set the capacity of the iSCSI drive during creation of a logical drive. Follow the steps below:

1. From the **Storage** tab, click **Logical Drive**.
2. Click the **Create Logical Drive** button.
3. Select the disk array you want to use and click the **Next** button.
4. In the **Create Logical Drive** window, complete the required settings:
   a. In the **Alias** field, enter an alias at a maximum of 32 characters (includes letters, numbers, space between characters, and underline).
   b. Set the **LDType** as *NAS* or *iSCSI Target*.
   c. Select a RAID Level from the drop-down menu. Available RAID options will depend on the number of physical drives in the disk array. (See “RAID Levels” on page 33.)
   d. In the **Capacity** field, accept the default maximum capacity or enter a lesser capacity (size in MB, GB or TB). Any remaining capacity is available for an additional logical drive.
   e. Choose the **Stripe** size: *64 KB, 128 KB, 256 KB, 512 KB*, or *1 MB*. (See “Stripe Size” on page 3333)
   f. Choose the **Sector** size: *512 B, 1 KB, 2 KB,* or *4 KB*. (See “Sector Size” on page 3333)
   g. Choose the **Read Policy**: *Read Cache, Read Ahead*, or *No Cache* (see “Stripe Size” on page 3333)
   h. Choose the **Write Policy**: *Write Back* or *Write Through*. (See “Write Policy” on page 3333)
   i. Click the **Add** button.
   j. The new logical drive appears in the **New Logical Drives** list. If there is capacity remaining, you can create an additional logical drive.
5. When done, click the **Submit** button. The new logical drive(s) will appear in the **Logical Drive** list. New logical drives are automatically synchronized if necessary. You can access the logical drive during synchronization, although performance may be slower than usual.
6. For logical drives configured as a NAS logical disk (LDType *NAS*) it is now necessary to create a file system. See the next page for instructions to continue setting up the logical drive.
7. Synchronization

Once you have finished creating a logical drive, the DataGuard Appliance will begin synchronization. The logical drive will be accessible during this process, but performance may be diminished. For more information on Synchronization, see page 53.



Storage > Logical Drive

Storage > Logical Drive > Create Logical Drive

Logical Drive Management

To view information about a logical drive and adjust parameters, follow these steps:

1. From the Storage tab, click the Logical Drive menu item. The list of logical drives will appear.
2. Move your pointer over the logical drive to display the available options.

- Click **View** to display information about a logical drive, or click Settings to change its configuration. The table below explains the meaning of each item in the information panel.
- Click **Settings** to change or delete the alias in the Alias field. You can also configure the Read Policy (ReadCache, ReadAhead, or NoCache) and Write Policy (WriteThru or WriteBack). Click the Save button to save and apply the settings.
- Click **Locate** to identify physical drives. This feature will make the status LEDs blink for one minute on all physical drives used in the disk array.
- Click **Delete** to remove a logical drive. If you choose this option it will be necessary to confirm the deletion in a new dialog. Click Confirm to delete the logical drive or Cancel to keep it.
- The **Check Table** option is used to display error tables used to evaluate the integrity of the logical drive and determine if any corrective action is needed.

Check Table Item	Description
Entry Number	A number assigned to each block of entry.
Table Type	Read Check, Write Check or Inconsistent Block.
Starting Logical Block Address	Logical block address (LBA) of the first block for this entry.
Count	Number of errors or continuous blocks starting from this LBA.
	Check Table display options
All	Display all errors
Read Check	Display Read errors
Write Check	Display Write errors.
Inconsistent Block	Display inconsistent blocks for this logical drive. Mirror data for RAID Levels 1, 1E and 10 or Parity data for RAID Levels 5 and 6. Identified by the Redundancy Check.

Warning
If you delete a logical drive, you also delete the data contained within it. Back up all important data before deleting a logical drive.

Logical Drive Information	Description
ID	Logical drive identifier: LD0, LD1, etc.
Alias	This is the alias assigned through the Logical Drive Settings menu.
Disk Array ID	Disk array identifier: DA0, DA1, DA2, etc.
RAID Levels	Lists the RAID level set when the logical drive was created.
Operational Status	Displays the current state of the logical drive.
Capacity	Displays the data capacity of the logical drive.
Number of Axles	1 axle for most RAID levels; 2 axles for RAID 10.
Physical Capacity	Capacity of the disk array used by the logical drive.
Number of Physical Drives	The number of physical drives in the disk array.
Stripe Size	Stripe size set when logical drive was created.
Read Policy	Adjustable in the Settings menu. See “Stripe Size” on page 3333.
Sector Size	Sector size set when logical drive was created.
Write Policy	Adjustable in the Settings menu. See “Write Policy” on page 3333.
Tolerable Number of Failed Drives	Number of physical drives that can fail without the logical drive going offline.
Synchronized	A new logical drive displays “No” until synchronizing is completed.
Codec Scheme	n/a
Serial Number	Unique number assigned to this logical drive.
LDType	Displays the LD type of the logical drive (NAS or iSCSI).

Logical Drive Problems

Logical drive problems typically result from physical drive failures such as a critical logical drive. The RAID controller can rebuild a critical logical drive. A more serious but less common problem is an Incomplete Disk Array, which results from a physical drive that fails or becomes missing during RAID level migration or physical drive transport.

Spare Drive

An unassigned hard drive can be assigned as a spare drive to replace a failed hard drive in a RAID volume. One that is active and connected is known as a “hot” spare drive.

- If a hard drive fails within a redundant RAID logical drive, and a spare drive is present, the system uses the spare drive to rebuild the array. Rebuilding begins automatically, and the spare drive becomes part of the RAID logical drive.
- The spare can be dedicated to a specified logical drive, or available to any logical drive when needed. If the spare is revertible, it will revert to spare status after the failed hard drive has been replaced and rebuilt.
- Some limitations on the use of spare drives with Imation DataGuard Appliances:

  ✓ A spare drive cannot replace a failed hard drive in a RAID 0 logical drive because of the way data is written to hard drives under RAID 0.

Storage > Spare Drive > Create Spare Drive (T5R)

Create Spare Drive

To assign a spare drive:

1. From the tab, click the menu item. If any spare drives are present, they will be displayed in a list here.
2. Click the button.
3. Click on an available physical drive in the diagram to select it as a spare drive. The ID numbers of the selected hard drive will appear in the field below the diagram.

- Choose the options for the hot spare drive. The *Revertible* option allows the spare drive to revert to hot spare status after a failed hard drive is replaced and rebuilt. At this point, the used spare drive will automatically be freed up and become a revertible spare again after the reversion process, called transition, is initiated and completed in the background.
- The can be *Global* or *Dedicated*. A *Global* spare is not dedicated to a specific RAID array, and remains available as a hot spare for any RAID array. A *Dedicated* spare drive is assigned to a specific RAID array. For most users, a *Global* and *Revertible* configuration is best.
- You can also enable when creating a spare drive. All these options can be changed after the spare is created.
- Click the button to designate the drive as a hot spare.

To change settings for an existing spare drive, click on the button for the listed spare and change the settings as desired.

Storage > Spare Drive > Create Spare Drive (R4)

File System

Create File System

If any part or all of a logical drive will act as a NAS, the drive must first have a file system. Follow the steps below to create a file system.

1. From the Storage tab, click the File System menu item. The File System panel will appear. This panel will display information about the Volume, Device ID, RAID Level, Capacity, Operational Status, File System, and whether the File System is Mounted.
2. Click on the row below these headings to view these additional options:

   ✓ Quota—Sets restrictions on user and group access

   ✓ Defragmentation—Rearranges data into contiguous blocks; can be scheduled

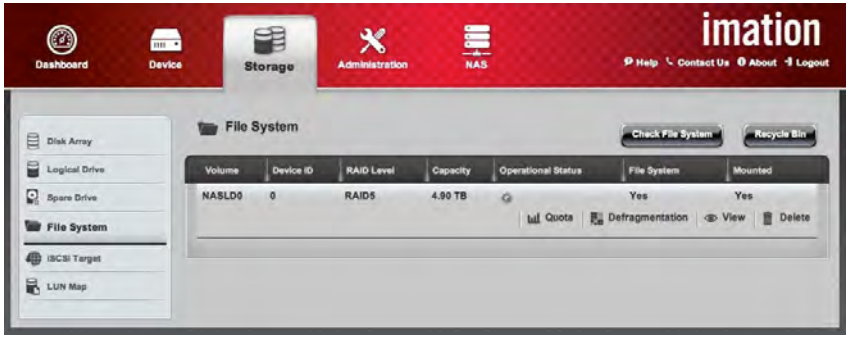
   ✓ View—Shows Volume, RAID Level, Operational Status, Capacity, Free Capacity, Used Capacity, and Usage; also lets administrator assign capacity or expand file system (if capacity allows)

   ✓ Delete—Allows administrator to delete all data on the selected file system

File System Options

- In the **File System** menu, set the capacity for the logical drive. The default capacity is 90% of the total available capacity. This is to allow adequate spare capacity for Snapshot Backups.
- If you decide to use encryption, you must provide the key when mounting the drive. To enable encryption on the logical drive, click to select the **Enable Encryption** option, enter and retype the **Encryption Key**.
- When **Mount Automatically** is enabled, the logical drive will be mounted after rebooting the device with the file system intact. If this feature is disabled, you will need to mount the logical disk manually.
- Use the **Check File System** button to check and correct file system errors.
- The **Recycle Bin** contains files deleted by users or the administrator. The Recycle Bin appears as a shared folder when enabled. Click the Empty button to clear the Recycle Bin.

Important
iSCSI devices will not be shown on this screen.



Storage > File System

Defragmentation

To perform or schedule defragmentation of the drives, do the following:

From the **Storage** tab, click **File System**. Move your pointer over row of the listed File System to reveal the Defragmentation option. Click the link to view the **Volume Defragmentation** menu.

1. To begin defragmentation, click the **Defragment** button. To schedule a defragmenting routine, choose the schedule option and configure the desired schedule. The options for scheduling are:
2. *Disable*—No defragmentation schedule
   - *Daily*—Defragmentation is scheduled each day at the time chosen from the drop-down menus.
   - *Weekly*—Defragmentation is scheduled each week at the day and time chosen from the drop-down menus.
   - *Monthly*—Defragmentation is scheduled each month at the day and time chosen from the drop-down menus.

User Quotas

An administrator can configure user quotas for the available data storage space on each logical drive.

1. From the **Storage** tab, click the **File System** menu. Move your pointer to expand the row for the logical drive you want to configure, and click on the **Quota** icon.
2. Enter an amount in Megabytes as the assigned data storage limit for each user in the corresponding Quota entry field. A value of 0 (the default value) means there will be no limit for that user. If the total available limit of storage is exceeded, an error message is displayed.

An additional option is available to set a “soft” quota for each user. The soft quota is set as a percentage of the total assigned quota for the user, when the set percentage of the quota is exceeded, an email alert is sent to the administrator.

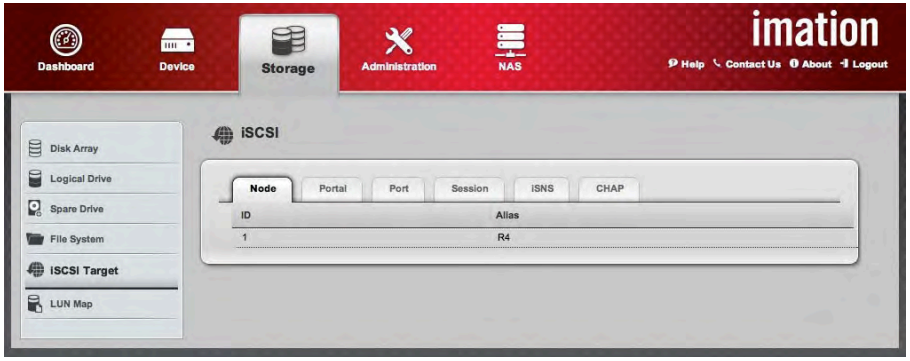
iSCSI Target

The iSCSI SAN protocol sends and receives SCSI commands over IP networks, making remote data storage facilities appear as local disks. Servers running iSCSI initiator software can use the DataGuard Appliance to access disk volumes. Use the iSCSI settings menu to configure these services.

Every Imation DataGuard Appliance supports use of iSCSI, functioning as a target or initiator. The R4 and T5R both support iSCSI boot service. The iSCSI features can be used with DHCP service and PXE to provide full-service boot up for properly equipped clients.

- Use the iSCSI Node Settings menu to configure iSCSI node (target) function.
- To configure iSCSI network booting, go to Administration > Service > iSCSI Boot Service.
- To configure LUN Mapping, go to Storage > LUNMap.
- To configure the DataGuard Appliance to function as an initiator, go to NAS > iSCSI Initiator.
- From the **Storage** tab, click **iSCSI Target** to display the iSCSI (Internet Small Computer System Interface) information in the system and configure iSCSI settings.

Important
An iSCSI SAN usually performs better if it is operating on a dedicated network, IP subnet, or VLAN.



Storage > iSCSI > Node

Menu	Description
Node	Displays information about the iSCSI function of the DataGuard Appliance, including Node Name, Role, Node Status, and other information. Click **Settings** to configure Node Name, Node Alias,,MaxBurstLength, TimeToWait, TimeToRetain, enable/disable Header Digest, enable/disable Data Digest, enable/disable Uni-directional CHAP Authentication, enable/disable Bi-directional CHAP Authentication, and NOP-IN.
Portal	Displays portal information including Portal ID, IP Address, TCP Port, Associated Type, and IF Name.
Port	Click View to show iSCSI port information including Controller ID, Port ID, Max Receive Data Segment Length, Number of Active Sessions and other information.
Session	Displays Session ID, Port ID and Device Name
iSNS	Displays Port ID, iSNS Status, Server IP Address and iSNS Port [1~65535]
CHAP	Configure CHAP or delete existing settings.
Ping	Perform standard Ping test for network connectivity.

iSCSI Node Settings

From the Storage tab, click **iSCSI Target > iSCSI > Node > Settings** to display the **iSCSI Node Settings** menu used for iSCSI target configuration.

The configuration settings are described in the table below.

Menu	Description
Node Name	This is the target name used by an initiator when logging on for iSCSI connection. A unique Node Name is generated automatically, however it can be changed here.
Node Alias	Name used for easy identification of the DataGuard Appliance on the network.
MaxBurst-Length	This is the maximum data payload in a sequence of Data-In or solicited Data-Out PDUs, in bytes, kilobytes or megabytes. A data sequence consists of one or more consecutive sequence of Data-In or Data-Out PDUs terminated with a Data-In or Data-Out PDU with the F bit set to one (finish flag). A Data-Out sequence is sent either unsolicited or in response to an request to transmit (R2T). This value is set when the initiator session is negotiated at login.
TimeToWait	The default time to wait is the minimum time, in seconds, to wait before attempting an explicit or implicit logout, or active iSCSI task reassignment after an unexpected connection termination or connection reset. The default is 2 seconds. If this is set to 0, an attempt to reconnect will happen immediately.
DefTimeTo Retain	This is the maximum time, in seconds after an initial wait (TimeToWait), before an active iSCSI task reassignment is possible after an unexpected connection termination or reset. The default is 20.
Enable Header Digest	When enabled, this increases data integrity by performing a checksum of each iSCSI Protocol PDU's header. Enabling this can affect iSCSI performance.
Enable Data Digest	When enabled, this increases data integrity by performing a checksum of each iSCSI Protocol PDU's data part. Enabling this can affect iSCSI performance.
Enable Uni-directional CHAP Authentication	This must first be enabled to use uni-directional CHAP for initiator authentication.
Enable Bi-directional CHAP Authentication	This must first be enabled to use bi-directional CHAP for mutual initiator/target authentication.
NOP-IN	Allows the initiator to issue a request for response from the target without requesting any other actions. This is used to ensure the connection is still alive or that the target is responsive.
Port ID	The Port Identifier is a Fibre Channel address identifier assigned to a node port or node loop port during fabric login.
iSNS Enable	Check to toggle on iSNS protocol support.
Server IP Address	The iSNS server responds to iSNS protocol queries and requests made by iSNS clients. Enter the IP address of a functioning iSNS server in the Server IP Address field.
iSNS Port [1~65535]	Choose the TCP port used for iSNS communications. The default iSNS protocol port is 3205.

iSCSI Port View

To display the read-only iSCSI Port settings, go to **Storage** > **iSCSI Target > Port**.

iSNS Port Settings

The Internet Storage Name Service protocol is used for automatic discovery of iSCSI devices as well as state change notification. iSNS servers can also store mappings of Fibre Channel devices to proxy iSCSI device images on the network. Use the iSNS Port Settings menu to enable iSNS and configure iSNS server IP and port settings.

Various iSCSI information can be viewed by clicking on the menus tabs and expanding the **View** menu. Some tabbed menus include **Settings** configuration menus.

iSCSI Session

From the **Storage** tab, click **iSCSI Target** > **Session** tab to display any active iSCSI sessions.

Important
iSCSI functions should be employed using security measures such as CHAP, Access Control and IPSec.

Note
To configure initiator access to disk volumes, Multipath I/O, CHAP or other initiator settings, please consult the documentation for your server or initiator software.

iSCSI CHAP

Challenge-Handshake Authentication Protocol (CHAP) is a security protocol used for authentication of iSCSI initiators, targets, or both. If CHAP is used, be sure to enable uni-directional or bi-directional CHAP authentication in the iSCSI Node Settings menu.

Setting up CHAP for iSCSI clients

1. From the **Storage** tab, click **iSCSI Target** > **CHAP**
2. Complete the required settings in the **Add CHAP** menu, then click the **Submit** button. The new user will appear listed below in a table of CHAP users.

To change the password for an existing CHAP user or to delete it, move your pointer over the **Setting** button to display the **CHAP Settings** menu.

CHAP Settings	Description
User Name	The user name used for CHAP authentication.
Password	This is the secret character string that is shared by the target and initiator but is not passed over the network. It functions as a user password.
Type	Choose to apply the user name and password to the peer seeking authentication or to the DataGuard Appliance (local) attempting to authenticate its identity.

Security Considerations for iSCSI

Any iSCSI SAN should be used with security measures to protect data in addition to segregating the iSCSI SANs from LAN traffic. To use any or all of the security measures supported by the DataGuard Appliance, make sure that the initiators also support use of CHAP (authentication), IPsec (encryption), Access Control and LUN mapping and LUN masking.

Network Considerations for iSCSI

The switches and network infrastructure connected to the DataGuard Appliance should be configured for best SAN performance. Use Gigabit Ethernet or faster switches. The configuration recommendations listed below apply to switch, connected ports and network configuration for the SAN.

- Disable unicast storm control (normally this is disabled by default on most switches)
- Enable Flow Control
- Enable Jumbo Frame support
- Turn off spanning tree
- Segregate SAN and LAN traffic
- Make sure the NICs used are Server class and preferably designed for storage

Important

CHAP implementation is used to verify the identity of iSCSI initiators and targets. It should be used together with other security measures such as Access Control and IPsec to provide more comprehensive data security.

LUN Map Management

The LUN Map function allows you to control which storage arrays are visible to specified computers as a means of access control for a SAN.

To enable LUN Mapping:

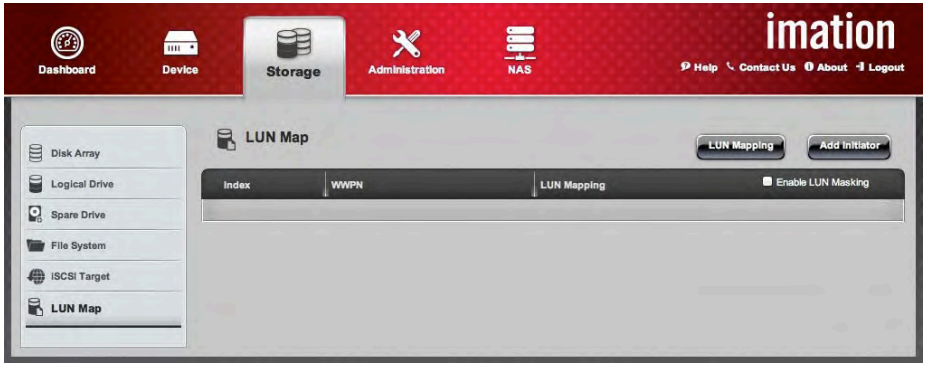
1. Check the **Enable LUN Masking** option.

To add an initiator:

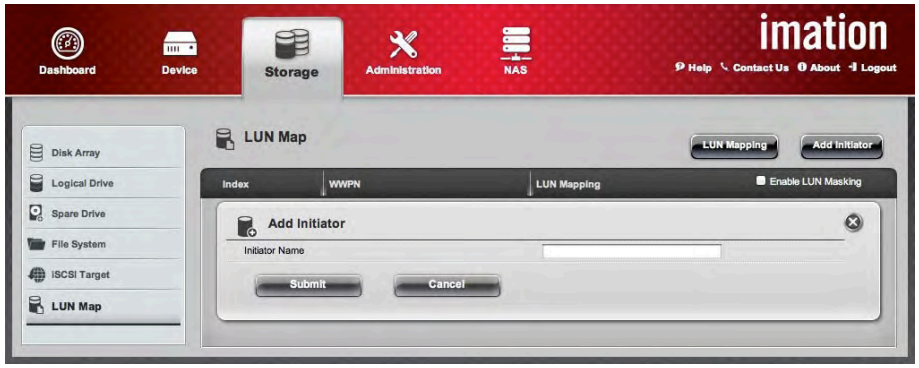
2. From the **Administration** tab, click the **LUN Map** menu item.
3. Click the **Add Initiator** button at the upper right of the panel.
4. Enter the full name in the **Initiator Name** field and click the **Submit** button.
5. Type the name of the initiator. An iSCSI initiator name is the iSCSI name of the initiator device and is composed of a single text string. Obtain the initiator name from the initiator utility on your host system. The newly added initiator will be added in the LUNMap list.

To define a LUN Map:

1. From the **Administration** tab, click the **LUN Map** menu item.
2. Click the **LUN Mapping** button.
3. Select an initiator from the drop-down menu, then click the **Next** button.
4. Drag-and-drop a logical drive from the Logical Drive pane to the Initiator pane.
5. In the **LUN Mapping** pane, indicate the arrays you wish to make visible by putting a unique number in the LUN field (on the Initiator pane).
6. When done, click the **Assign** button.
7. Click the **Submit** button.



Storage > LUN Map



Storage > LUN Map > Add Initiator

Note
The initiator name you input must match exactly in order for the connection to work.

Administration Tab

Subsystem Information

The Administration tab enables you to manage the DataGuard Appliance subsystem, monitor events, manage background activities, perform firmware updates, restore factory default settings, and save a configuration report. Available system information includes:

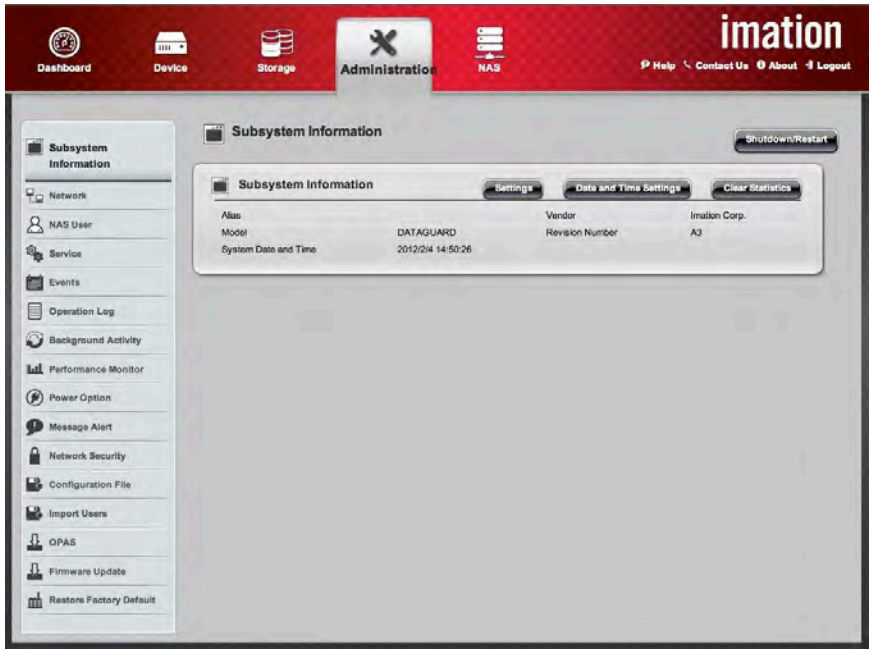
- Alias (if assigned)
- Vendor
- Model
- Revision Number (of controller board)
- System Date & Time

To change Subsystem settings:

1. From the **Administration** tab, click the **Subsystem Information** menu item. A pane will open with three buttons: **Settings, Date and Time Settings,** and **Clear Statistics.**
2. Click the **Settings** button.
3. In the **Alias** field, enter an alias or change the existing alias, then click the **Save** button.
4. Click the **Date and Time Settings** button. You can set the date and time manually, or by synchronizing the clock and calendar with an NTP service.

   ✓ To set the date and time manually, click the Date and Time Settings folder tab. Use the date field and pull-down menus to set the correct date and time, then click Save to apply the new settings.

   ✓ To synchronize with an NTP service, click the NTP Management folder tab. Select an NTP server and schedule, then click the Save button.



Administration > Subsystem Information

5. To clear statistics on controllers, physical drives, and logical drives, click the **Clear Statistics** button. Click **Confirm** to clear all information.

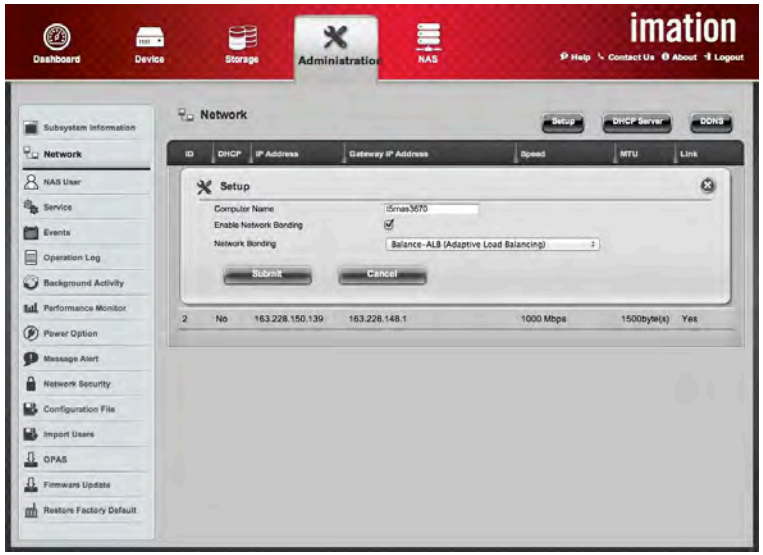
To shut down or restart the Subsystem:

1. Click **Administration** tab > **Subsystem Information**.
2. Click the **Shutdown/Restart** button above the Subsystem Information panel.
3. In the **Shutdown/Restart** window, you can:

- Click the **Shutdown** button to stop I/O and shut down the subsystem.
- Click the **Restart** button to stop I/O and restart the subsystem.

Network

TCP/IP Settings	Description
Network Speed	Options are Max Supported Speed and 100 Mbps.
DHCP	When enabled, all IP settings will be assigned by a DHCP server. When disabled, IP settings need to be configured manually using the remaining entry fields.
IP Address	The IP address of the network interface. If entering this manually make sure IP address fits with the network IP addressing and subnetting scheme. Separate subnets may be used for NAS devices to improve efficient use of available network bandwidth.
Subnet Mask	IP subnet mask.
Gateway IP Address	IP address of router, or gateway IP device used for access to the subnet.
DNS Server IP Address	DNS server IP address.
Secondary DNS Server IP Address	Auxiliary DNS server IP address.



Administration > Network > Setup

Network Bonding

Network bonding is used to control how the network interfaces manage traffic when both are connected to a switch and active. The connected switch ports must be configured with identical bonding settings. Use this to configure the Device Name and network bonding:

1. From the Administration tab, click **Network**, then click the **Setup** button.
2. Complete the required settings in the **Setup** window, and then click the **Submit** button.

Network Settings	Description
Computer Name	Shows the name of the DataGuard Appliance as it appears on the network.
Enable Network Bonding	Enables the selected network bonding mechanism.
Network Bonding	Allows you to choose one of the following options: **Balance-alb** (Adaptive Load Balancing): Supports transmit load balancing and receive load balancing for IPV4 traffic; does not require special switch support. Receive load balancing is achieved by ARP negotiation. The bonding driver intercepts ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server. **Balance rr** (Round Robin): Transmits packets in sequential order from the slave. This mode provides load balancing and fault tolerance. **Active Backup** (Fail Over): If the slave interface fails, the remaining master interface becomes the fail over port. The bond's MAC address is externally visible on only one port to avoid confusing the switch. This mode provides fault tolerance. **Balance XOR**: Transmit based on [(source MAC address XOR'd with destination MAC address) modulo slave count]. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance. **Broadcast**: Transmits everything on the slave interface. Provides fault tolerance. **802.3ad**: IEEE 802.3ad Dynamic link aggregation aka LACP. Creates aggregation groups that share the same speed and duplex settings. Uses the slave in the active aggregator according to the 802.3ad specification.

DHCP Server Function

The DataGuard Appliance includes an embedded DHCP server that can be used to function on the subnet or dedicated network to which it is attached. Make sure it is appropriate or desirable to enable DHCP service before using it. To configure DHCP Server Settings:

1. From the **Administration** tab, click the **Network menu** item, then click the **DHCP Server** button.
2. Check the **Enable DHCP Server** button to activate.
3. Enter a value for the **IP Range.**
4. Set a **Lease Time** for the period you want the server to remain active.
5. Click **Submit** to apply the new settings, or click **Cancel** to return to the previous settings.

DHCP Server Settings	Description
Enable DHCP Server	Choose to enable or disable DHCP service on the attached network or subnet.
IP range	Assign a suitable range of IP address to use for DHCP assignment in the text boxes.
Lease Time	Choose the amount of time allowed for IP address leasing.

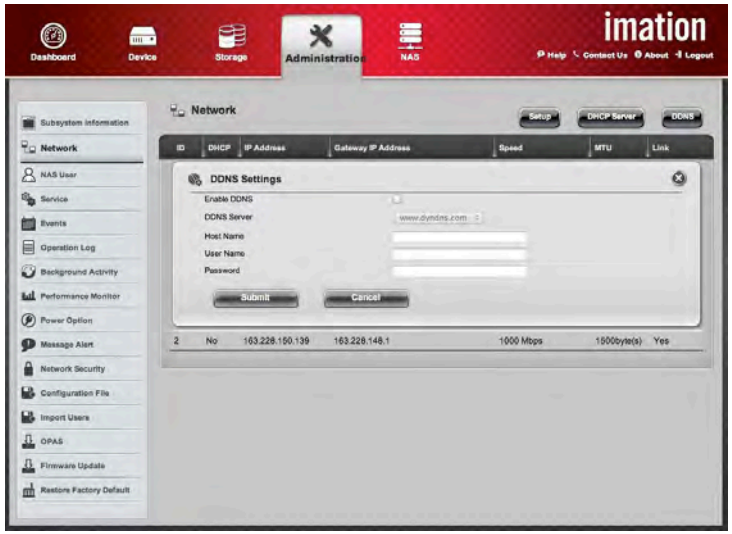
Administration > Network > DHCP Server Settings

Setting up DDNS

DDNS can be used to maintain and update DNS information to make the system easier to locate from the web.

1. From the **Administration** tab, click the **Network menu** item.
2. Click the **DDNS Settings** button.
3. Select a DDNS server from the drop-down menu and enter a Host Name, User Name, and Password.
4. Click the **Submit** button.

DDNS Settings	Description
Enable DDNS Server	Choose to enable or disable DDNS service.
DDNS Server	Choose a DDNS service domain from the listed websites.
Host Name	Enter the host name used for DDNS service.
User Name	Enter the user name used for DDNS service.
Password	Enter the password used for DDNS service.



Administration > Network > DDNS Settings

TCP/IP Settings

1. From the **Administration** tab, click the **Network menu** item, then click the **TCP/IP Settings** button.
2. Select a **Network Speed** from the pull-down menu.
3. To set IP Properties, choose one of two methods:

   ✓ Check the box marked Obtain an IP Address automatically; or

   ✓ Enter a fixed (static) IP Address, Subnet Mask, Gateway IP Address, DNS Server IP Address, and Secondary DNS Server IP Address in the fields provided.
4. Click the **Submit** button to apply these settings.

Administration > Network > TCP/IP Settings

IPv6 Settings

To configure the DataGuard Appliance for use with the IPv6 protocol, follow these steps:

1. From the **Administration** tab, click the **Network menu** item, then click the **IPv6 Settings** button.
2. Select a **Network Speed** from the pull-down menu.
3. Check the **Enable Service** box.
4. To set IP Properties, choose one of two methods:

   ✓ Check the box marked Obtain an IP Address automatically; or

   ✓ Enter a fixed (static) IPv6 Address, Subnet Mask, Gateway IP Address, DNS Server IP Address, and Secondary DNS Server IP Address in the fields provided.
5. Click the **Submit** button to apply these settings.

MTU Settings

If your network is configured to use maximum transmission unit (MTU) , you can set the DataGuard Appliance to take advantage of its capabilities. Follow these steps:

6. From the **Administration** tab, click the **Network menu** item, then click the **MTU Settings** button.
7. Confirm that the **Ethernet Link Mode** and **Ethernet Link Speed** are correct.
8. Select a maximum transmission utin from the pull-down menu.
9. Click the **Submit** button to apply these settings.

NAS User

Manage User and Group Accounts

To add a new NAS User:

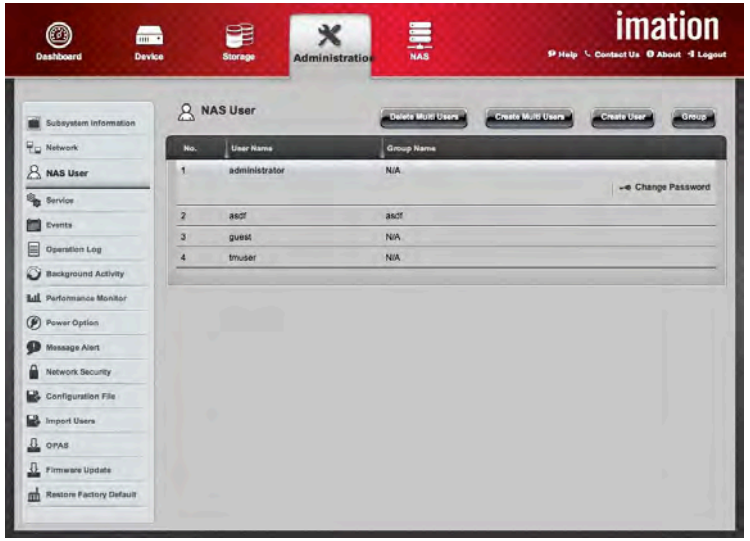
1. From the **Administration** tab, click the **NAS User** menu item.
2. Click the **Create User** button. In the Create User window, complete the required settings:
   - ✓ User Name
   - ✓ Password
   - ✓ Retype Password
   - ✓ Permissions (Deny-Access, Read-Only, Read-Write)
3. Click the **Save** button to apply and save the settings.

To view or edit NAS User information:

1. From the **Administration** tab, click the **NAS User** menu item to display a list of users.
2. Move your pointer over the user in the list to reveal configurable options.
3. To change the user's login password, click the **Change Password** button.
4. To remove the selected user, click the **Delete** button.

Note
To configure Active Directory users and groups, see domain settings on page 74.

Note
The user listed as Administrator cannot be deleted.



Administration > NAS User

To create a new NAS Group:

1. From the **Administration** tab, click the **NAS User** menu item to display a list of users.
2. Click the **Group** button, then click the **Create Group** button.
   - ✓ Enter a Group Name, then click Next.
   - ✓ Select the users you want to add to the group from the NAS User field.
3. When you are finished adding group members, click the **Submit** button.

To view or edit NAS Group information:

In the NAS Group list, move your pointer over the group item. To remove groups, click the **Group Settings** button, then select the group you want to remove and click the **Delete** button.

Administration > NAS Group > Create Group

To add multiple new NAS Users:

1. From the **Administration** tab, click the **NAS User** menu item.
2. Click the **Create Multi Users** button. In the Create Multi Users window, complete these fields:
   - ✓ Start Index (number appended to user name)
   - ✓ Quantity (number of users to create)
   - ✓ User Name (prefix)
   - ✓ Password
   - ✓ Retype Password
   - ✓ Permissions (Deny-Access, Read-Only, Read-Write)
3. Click **Save** to apply the settings, or click **Cancel** to leave the previous settings in place.

To delete multiple NAS Users:

1. From the **Administration** tab, click the **NAS User** menu item.
2. Click the **Delete Multi Users** button.
3. Select the users to be removed by clicking the box next to each user name to be deleted.
4. Click the **Delete** button to apply the settings.

Administration > NAS User > Create Multi Users

Service

Use the various Service options to configure settings for standard network functions such as **Telnet**, **SSH**, **SNMP**, as well as **PXE Service**, **Web Virtual Hosting** and **iSCSI Boot Service**. To view the available categories:

1. From the **Administration** tab, click the **Service** menu item.
2. Move your pointer over the name of any service in the list to reveal the **Start** or **Stop** commands; some services also have configurable options.
3. Click the **Start** icon to enable a service; click the **Stop** icon to disable it.

Telnet

Use the Telnet Settings menu to change the port used for telnet connections. The default port on the DataGuard Appliance for Telnet is 2380 (the standard port for Telnet is 23).

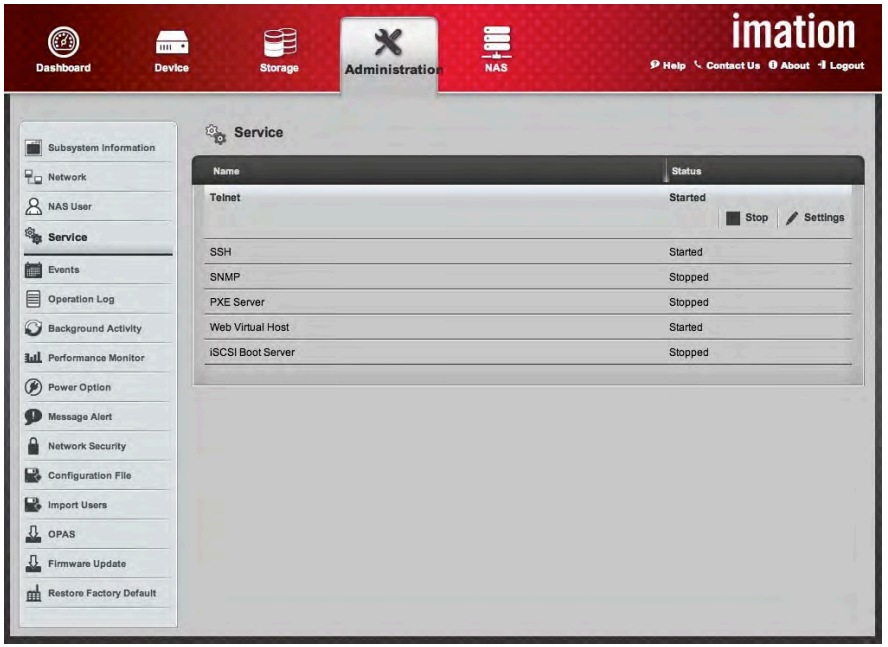
SSH

Use the SSH Settings menu to change the port used for Secure Shell (SSH) connection. The default port used on the DataGuard Appliance is 22 (also the standard port for SSH).
SNMP
Move your pointer over the SNMP row to reveal links to the SNMP configuration menus (SNMP **Settings** and **Trap Settings**), as well as the **Download MIB** and **Start/Stop** (SNMP) icons.

SNMP is not enabled by default. Click the **Start** icon to begin SNMP function. Use the **Settings** to configure SNMP settings including **Port** (default is standard port 161), **System Name**, **System Location**, **System Contact** information, **Read Community** and **Write Community**.

Use the **Trap Settings** menu to set the level of notifications for **Trap Receivers** specified by IP address. The notification levels are *Info*, *Warning*, *Minor*, *Major*, *Critical* and *Fatal*; these are set using the **Trap Filer** pull-down menu. To add a trap setting, enter the IP address of the **Trap Receiver**, choose the **Trap Filter** to set the level of trap warning, and click on the **Add** button.

To download the device MIB file used for SNMP, click the **MIB Download** icon and follow the instructions of the menu prompts for your OS to place the MIB.



Administration > Service

PXE Server

The DataGuard Appliance supports Preboot Execution Environment (PXE) service to provide a boot environment for remote systems and diskless nodes. PXE can be used with the embedded iSCSI Boot and DHCP Servers to provide full-service boot up for iSCSI client systems. Use the PXE Server **Settings** menu to enable PXE, define the **Share Folder** used to store the boot file and the **File Name** of the boot file. Click on the **Submit** button to commit the settings. The service must then be started by clicking on the **Start** button. The default file name is the standard **pxelinux.0**, but can be changed to any legal file name for a boot file.

iSCSI Boot Server

The iSCSI boot service, together with DHCP service and PXE, are used to provide full-service boot up for properly equipped iSCSI clients. Typically the iSCSI client will be an initiator or diskless client running iSCSI booting software. To use the iSCSI Boot Server feature, follow these instructions:

1. Click the Administration tab > Service > iSCSI Boot Server.
2. Click to check the Enable Services option box.
3. Choose the Mode of the server for Single or Multiple client systems.

Web Virtual Host

The Web Virtual Host Settings option lets you create one or more embedded web hosts on the DataGuard Appliance. A web host allows the DataGuard Appliance to function as a web server for public web site hosting or web services that can be delivered by HTTP to a client browser connecting to the device from the Internet.

Before the web host can function as a public web server, you will need a registered domain name to allow access by a browser, and the global IP should either be a static IP address (recommended), or a dynamic IP address with Dynamic DNS (DDNS or DynDNS) to match the domain name URL with the global IP.

Files used for the web pages (HTML, CSS, etc) must be stored in a folder within the WWW folder on the DataGuard Appliance. In Web Virtual Host Settings menu, enter the registered domain name, the name of the web files folder, and a port number between 1025 and 65535 for the connection.

To create a Web Virtual Host, follow these steps:

1. Obtain a static IP address from your internet service provider for the Internet connection the host will use; if you have a dynamic IP address, use a Dynamic DNS service.
2. Register the domain name or names used for the web host connection. For example, the domain name “site-one” and the common top-level domain “.com” create a URL of “site-one.com”.
3. Create a folder for web documents within the WWW folder. Use the domain name (“site-one” in this example) as the name of this folder.
4. From the Administration tab, click Service, then Web Virtual Host, then Settings to view the Web Virtual Host Settings menu. Click the Enable Services check box .
5. Enter the registered domain name (“site-one.com” in this example) in the Host Name field. Do not enter “www” or a subdomain of the URL; that is already listed as part of the file path.
6. In the Folder Name field, enter the name of the web document folder inside the WWW folder (“site-one” in this example) on the DataGuard Appliance.
7. Enter a valid port number between 1025 and 65535 in the Port field. This is the port that will be open to allow incoming file sharing connections.
8. Click the Add button to add the host name to the list, then click the Save button.
9. Check to make sure the service is “Started” by looking at the status listed under Web Virtual Host in the Service menu.
10. To add an additional web host, click the Settings button under Web Virtual Host in the Service menu and repeat the setup steps.
11. When the web host is set up correctly and the folder contains the web documents needed to render the web pages and content, users can connect to the web site and display the content in their browser.

To access web content at the site-one domain, enter “http://site-one.com:9999” and press the Enter key. The DNS service will match the domain name site-one.com to the IP address for the web host server Internet connection. The DataGuard Appliance will then use the designated port 9999 to direct the incoming connection to the correct subfolder in the WWW folder.

- If the port number 9999 is not entered in the URL, the incoming connection will use the default HTTP port 80, and the client will be directed to the DataGuard Management Interface.
- HTTP connections can be controlled for security using Network Security options (Administration > Network Security).
- Incoming Internet connections will be subject to any policies being implemented on a gateway device, such as a router or firewall, between the DataGuard Appliance LAN connection and the WAN connection.

Note

The WWW folder can be accessed through File Sharing (see page 77) or by using the Web File Manager plug-in (see page 78).

Events

Runtime events are the most recent events since the last DataGuard Appliance startup. These are useful for auditing usage, identifying trends, and tracing problems. The Management Interface also displays NVRAM event logs, which remain available even after a restart.

To view Runtime Events or NVRAM Events:

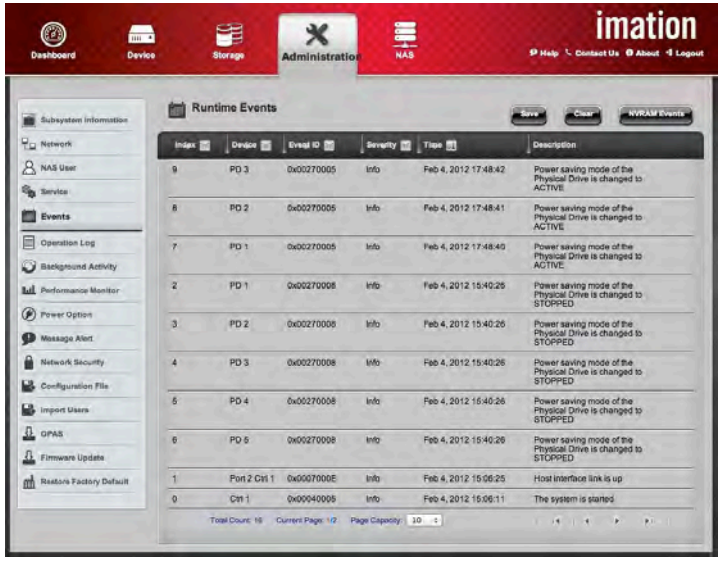
1. From the **Administration** tab, click the **Events** menu item.
2. Click the button at the upper right to toggle between Runtime Events and NVRAM Events.

To save the Runtime Events or NVRAM Events log:

1. From the **Runtime Events** or **NVRAM Events** panel, click the **Save** button. Your web browser will save a text file of the log to its designated download folder.

To clear the Runtime Events or NVRAM Events log:

1. From the **Runtime Events** or **NVRAM Events** panel, click the **Clear** button. A dialog box will appear.
2. Type the word “CONFIRM” in the dialog box and click Confirm to apply the changes, or click Cancel to keep the log intact.



Administration > Events > Runtime Events

Operation Log

The Operation Log lists changes that have been made to device configuration settings, array setup, logical drive setup and other significant management changes made through the API. To view the Operation Log:

1. From the **Administration** tab, click the **Operation Log** menu item.
2. Click on the **Time, API,** and **Description** table headings to sort the listed entries.

By default, the log is displayed in reverse order of the entry index number. The list of Runtime or NVRAM Events displays information that includes the following:

Event log item	Description
Index	A number assigned to this specific event. Highest number is most recent.
Device	Identifies the device involved.
Event ID	Identifies the action that occurred.
Severity	Displays the Severity Level: Fatal – A non-recoverable error or failure has occurred. Critical – Action is needed now; the implications of the condition are serious. Major – Action is needed now. Minor – Action is needed but the condition is not serious yet. Warning – User can decide whether action is required. Info – Information only; no action is required.
Time	Date and time the event occurred.
Description	A brief description of the event.

Background activity

Background activity includes monitoring for data integrity and hard drive performance. To see which processes are active, and to configure others for use, click the Background Activity menu item on the Administration tab. You will then have access to the following functions:

Media Patrol

Media Patrol monitors the condition of the media, not the data recorded on the media. This routine maintenance procedure checks the magnetic media on all physical drives assigned to disk arrays and spare drives; it does not check unconfigured drives. Media Patrol is enabled by default on all disk arrays and spare drives. Disabling is allowed but not recommended. If Predictive Data Migration (PDM) is enabled on the disk array and Media Patrol encounters a critical error, Media Patrol will trigger PDM. Media Patrol has three status conditions:

- **Running—**Normal. You can access your logical drives at any time.
- **Yield—**Temporary pause while a read/write operation takes place.
- **Paused**—Temporary pause while another background runs, or a pause initiated by the user.

Redundancy Check

Redundancy Check is a routine maintenance procedure for fault-tolerant logical drives, ensuring that all data matches exactly. It can also correct inconsistencies. To run Redundancy Check on a logical drive:

1. From the **Administration** tab, click the **Background Activity** menu item.
2. Move your pointer over the **Redundancy Check** item and click the **Start** button.
3. Check the boxes to the left of the logical drives you want to run, then check the options you want:

- Auto Fix—Attempt to repair the problem when an error is found
- Pause on Error—Stop the process stops when a non-repairable error is found

4. Click the **Confirm** button.

While the redundancy check is in progress, you can stop, pause or resume the process. Move your pointer over the buttons for these options, and click to activate.

Rebuild

When a physical drive in a disk array fails and a spare drive of adequate capacity is available, the disk array begins to rebuild automatically using the spare drive.

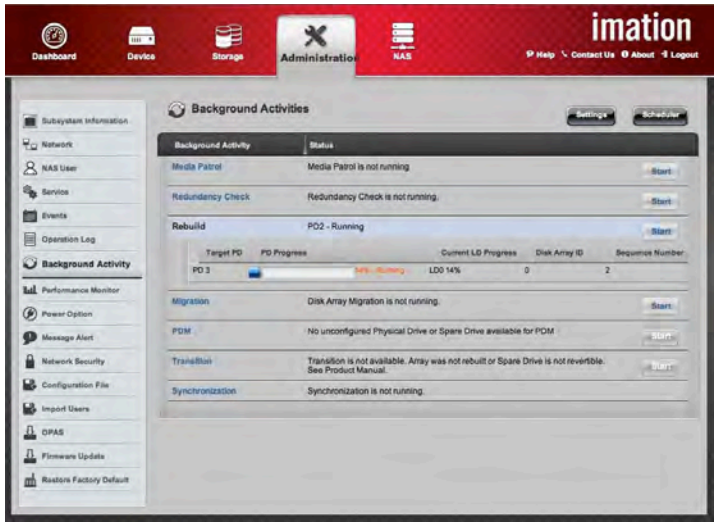
- If the Auto Rebuild function is enabled but there is no suitable spare drive, the disk array begins to rebuild automatically as soon as you remove the failed physical drive and install an unconfigured physical drive in the same slot.
- If the Auto Rebuild function is disabled and there is no suitable spare drive, you must replace the failed drive with an unconfigured physical drive, then perform a Manual Rebuild.

Migration

Migration means changing the RAID level of a logical drive, expanding the storage capacity of a logical drive, or both. Before you begin a migration, examine your current disk array to determine whether:

- The physical drives in your array can support the target RAID level
- There is sufficient capacity to accommodate the target logical drive size

If you need to add physical drives to your array, be sure you have unassigned physical drives installed in your DataGuard Appliance before you begin migration.



Administration > Background Activity

Predictive Data Migration (PDM)

PDM is the migration of data from a suspect drive (a drive with bad sectors) to a spare drive. Unlike Rebuilding, PDM constantly monitors drives and automatically copies data to a spare drive *before* the suspect drive fails and the logical drive goes Critical. PDM also counts the number of media errors reported by Media Patrol. The following actions trigger PDM:

- A hard drive is detected with unhealthy status, such as when a SMART error is reported or the bad sector remapping table fills to the specified level
- Media Patrol finds a disk critical error
- You initiate PDM manually

You can specify maximum levels for reassigned and error blocks in PDM settings. When the table fills to a specified value, PDM triggers a data migration from the suspect drive to a replacement physical drive.

Logical drives are accessible during data migration, but they respond more slowly to read/write tasks. The time required for data migration depends on the size of the hard drives. PDM is enabled on all disk arrays by default. Disabling PDM is possible but not recommended.

Transition

Transition is the process of replacing a revertible spare drive that is currently part of a disk array with an unconfigured physical drive or a non-revertible spare. The revertible spare drive returns to its original status. In order to run the Transition function, the spare drive must be revertible. In addition, you must specify an unconfigured physical drive of the same or larger capacity and same media type as the revertible spare drive.

Synchronization

Synchronization recalculates the redundancy data to ensure that the working data on the physical drives is properly in sync. To see whether a drive has been synchronized, follow these steps:

1. From the **Administration** tab, click the **Background Activity** menu item.
2. Move your pointer over the **Synchronization** row and click on the **View** button for a logical drive.
3. Look under Logical Drive Information beside the line that says Synchronized. “Yes” means the logical drive was synchronized.

To change Synchronization settings, follow these steps:

1. From the **Administration** tab, click the **Background Activity** menu item.
2. Click the **Settings** button.
3. Click the **Background Synchronization Rate** drop-down menu and choose a rate:

- Low—Fewer system resources to Synchronization, more to data read/write operations.
- Medium—Balances system resources between Synchronization and data read/write operations.
- High—More system resources to Synchronization, fewer to data read/write operations.

4. Click the **Confirm** button.

Background Activity Schedule Setup

The background activities **Media Patrol**, **Redundancy Check** and **Spare Check** can be scheduled during off-peak hours. To add a scheduled background activity:

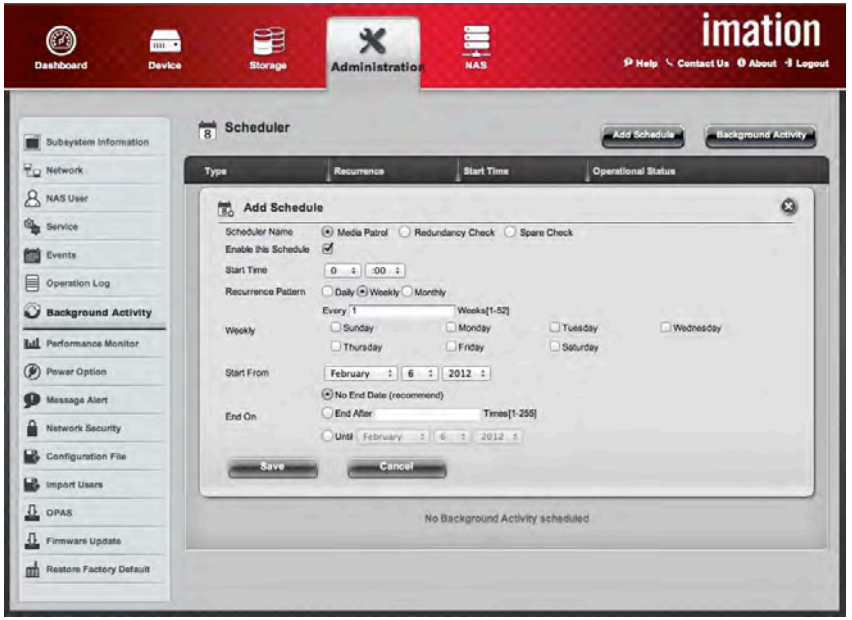
1. From the **Administration** tab, click the **Background Activity** menu item.
2. Click the **Scheduler** button.
3. Click the **Add Schedule** button and complete these settings:

Schedule Item	Description
Scheduler Name	Select the option to schedule: Media Patrol, Redundancy Check, or Spare Check.
	If you select Redundancy Check, complete the following settings: • Auto Fix—Attempts to repair the problem when it finds an error. • Pause on Error—The process stops when it finds a non-repairable error. • Select LD—Select at least one logical drive on which Redundancy Check will run.
Enable This Schedule	Click to toggle enable/disable of the schedule.
Start Time	Choose the time of day on which to begin the scheduled task.
Recurrence Pattern	Choose to establish a schedule pattern on a Daily, Weekly or Monthly basis. The menu changes according to the pattern chosen. Complete the schedule using the appropriate menu.
Start From	Select the date on which the scheduled activity is to begin.
End On	Choose one of the options to discontinue the activity. The options are: • No End Date—the activity continues indefinitely, • End After—choose a fixed number of times to perform the activity, or • Until—choose to continue the activity until a specified date.

Click the **Save** button to save and apply the schedule.

To change a scheduled background activity:

1. From the **Administration** tab, click the **Background Activity** menu item.
2. Click the **Settings** button.
3. Make the changes and click the **Confirm** button.



Administration > Background Activity > Add Schedule

Background Activities Settings

Background activities can be configured to use more or fewer system resources. Settings should be balanced according to network demands. If the DataGuard Appliance will be heavily used, for example, performance will be a higher priority. The rates for the various background activities are:

- Low—Fewer system resources to the rebuild, more to data read/write operations.
- Medium—Balances system resources between the rebuild and data read/write operations.
- High—More system resources to the rebuild, fewer to data read/write operations.

The following table shows available settings for background activities:

Activity Setting	Description
Rebuild Rate	This is controls the speed of rebuilding a new physical drive that replaces a failed physical drive. The default is High.
Background Synchronization Rate	This controls the speed of background synchronization. The default is Low.
Logical Drive Initialization Rate	This controls the speed of logical drive initialization. The default is Medium.
Redundancy Check Rate	This controls the speed of logical drive initialization. The default is Medium. Note that redundancy checking can be done during off hours using the Scheduler.
Migration Rate	This controls the speed of RAID level migration (i.e. changing the type of RAID). The default is *High*. Note that RAID level migration is typically very slow even at the highest rate, and has a large impact on device performance.
PDM Rate	Predictive Data Migration is a process that is triggered if the Media Patrol operation detects too many errors (as determined by the Reassigned Block Threshold and Error Block Threshold). Use this to control the rate of that migration. The default level is High.
Transition Rate	The Transition Rate controls speed at which a revertible disk that is part of an array goes through the process of transition back to spare drive status. The default rate is Medium.
Reassigned Block Threshold	When an error occurs in a physical drive, the directions to the block containing the error are reassigned. When the number of reassigned blocks exceeds the threshold, PDM is triggered.
Error Block Threshold	When an error occurs in the data or the physical media in a disk drive, the block is marked and added to the block error count. When the number of error blocks exceeds the threshold, PDM is triggered.
Enable Media Patrol	Media Patrol is enabled by default. Use this option to toggle enable/disable for Media Patrol.
Enable Auto Rebuild	Auto Rebuild is the function that rebuilds a hard disk drive when you swap out a failed drive with a new one.

Administration > Background Activity > Settings

Performance Monitor

The Performance Monitor screen allows you to monitor the performance of the DataGuard Appliance using graphical information.

Performance Category	Logical Drive	Physical Drive	Port
Bandwidth	✓	✓	✓
Cache Usage	✓		
Dirty Cache	✓		
Maximum Latency	✓	✓	✓
Average Latency	✓	✓	✓
Minimum Latency	✓	✓	✓
IO request	✓	✓	✓

To view Logical Drive performance:

1. From the **Administration** tab, click the **Performance Monitor** menu item.
2. In the **Logical Drive** field, click the **Select Logical Drives** button to select the logical drive you want and select a performance type from the drop-down menu. Performance information for the selected logical drive will be shown in the panel.

To view Physical Drive performance:

1. From the **Administration** tab, click the **Performance Monitor** menu item.
2. In the **Physical Drive** field, click the **Select Physical Drives** button to select the physical drive you want and select a performance type from the drop-down menu. The performance of selected physical drives will be shown in the panel.

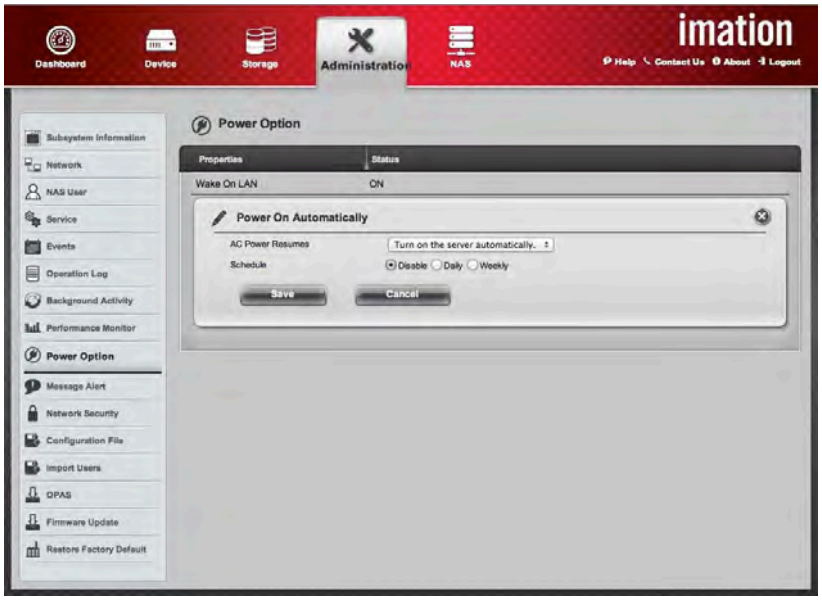
To view Port performance:

1. From the **Administration** tab, click the **Performance Monitor** menu item.
2. In the **Port** field, click the **Select Ports** button to choose a port and select a performance type from the drop-down menu. The performance of selected port will be shown in the panel.

Power Option

The Power Option panel displays power management settings for the DataGuard Appliance. To configure these options:

1. From the **Admnistration** tab, click the **Power Option** menu item.
2. Move your pointer over **Wake On LAN** and click the **Settings** option.
3. To activate Wake On LAN, check the **Enable Services** box, then click the **Save** button.
4. Move your pointer over **Power On Automatically** and click the **Settings** option.
5. Select a setting for **AC Power Resumes** from the drop-down menu.
6. Select a schedule (Disable, Daily, Weekly) from the radio buttons. Use the pull-down menus to specify times and dates, then click the **Save** button.



Administration > Power Option

Message Alert

The DataGuard Appliance can be configured to send e-mail or SMS alerts when certain events occur.

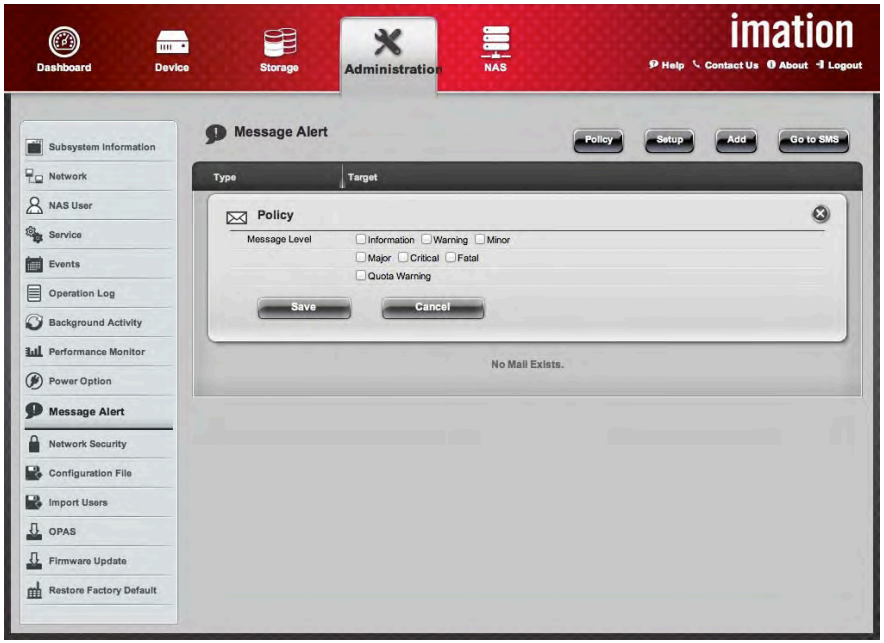
To set up e-mail alerts:

1. From the **Administration** tab, click the **Message Alert** menu item.
2. Click the **Policy** button, then check the boxes for which alerts you want to send. Click the **Save** button to apply the new settings.
3. Click the **Add** button, then enter an e-mail address for the intended recipient. Click the **Save** button. You can also edit or delete e-mail addresses from this panel.
4. Click the **Setup** button to reveal the settings panel. Check the **Enable Services** box, then fill in the remaining fields for sending messages. See the table below.
5. Click the **Test** button to send a test message; click the **Save** button to apply the new settings, or click the **Cancel** button to leave this feature inactive.

To set up SMS alerts:

1. From the **Administration** tab, click the **Message Alert** menu item.
2. Click the **Policy** button, then check the boxes for which alerts you want to send. Click the **Save** button to apply the new settings.
3. Click the **Go to SMS** button, then click the **Add** button.
4. Select a Country Code from the pull-down menu and enter a number in the Cell Phone Number field.
5. Click the **Add** button to confirm your choice, or click the **Cancel** button to leave the SMS settings unchanged.

Alert Item	Description
Enable Services	Check to enable message alert service.
SMTP Server	Enter the IP address of SMTP server.
SMTP Port	Enter the port number of SMTP server.
From	The sender of the notification message.
SMTP Authentication	Check to enable or disable.
Username	Enter the username to log in the SMTP server.
Password	Enter the password to log in the SMTP server.



Administration > Message Alert > Policy

Network Security

Network Security Policy determines how access to the DataGuard Management Interface is handled. Access Protection enables and configures secure connections, implements block policies for IP addresses that fail the secure connection challenge, and determines which connection protocols are allowed.

To set up Security Policy:

1. From the **Administration** tab, click the **Network Security** menu item, then click the **Security Policy** button and complete these settings:

- **HTTPs Redirection—**Redirects incoming HTTP connections to the more secure HTTPs protocol. Options are **All (**all HTTP connections including local network), or **Internet Connection Only** (only HTTP connection from the Internet). The default is **Never** (disabled).
- **I/O Policy**—Allows or denies access to specified IP addresses. For **Allow IP,** type the IP address or addresses that are allowed to connect. These will be the only IP addresses that can connect to the DataGuard Management Interface. Include the IP address of the system currently being used. For **Deny IP,** type the IP address or addresses that are NOT allowed to connect. Any IP address *not* listed will be allowed. The default is **Allow All** (any IP address can connect).

✓ To enable administrative access over the Internet, check the Allow Administrator from Internet button.

✓ To enable administrative login over SSH/Telnet, check the Allow Root Login By SSH/Telnet button.

2. When done, click the **Save** button.

Administration > Network Security > Security Policy

To set up Access Protection:

1. From the **Administration** tab, click the **Network Security** menu item, then click the **Access Protection** button and complete these settings:

- **Enable Services**—Check to enable the Access Protection as configured in this menu.
- **Block Policy**—Determine how to handle a failed login.
- **Protocol—**Choose which connection protocols to enable.

2. When done, click the **Save** button.

To set up SSL Certificate:

1. From the **Administration** tab, click the **Network Security** menu item, then click the **SSL Certificate** button and complete these settings:

- **Specific SSL Certificate—**Check to enable the function.
- **Certificate** (X.509 format)
- **Private Key** (X.509 format)

2. When done, click the **Save** button.

Configuration File

This feature lets you export configuration files for use in other installations, or as backup files for restoration in case of failure. To import or export a system configuration file, follow these steps:

To import an existing configuration file:

1. From the **Administration** tab, click the **Configuration File** menu item.
2. Click **Import** on the panel.
3. Click the **Browse** (or **Choose File**) button. Locate the correct configuration file (.bcf), then click the **Open** button.
4. Click the **Submit** button. The DataGuard Appliance will reboot.

To export the current configuration file:

1. From the **Administration** tab, click the **Configuration File** menu item.
2. Click **Export** on the panel.
3. Click the **Submit** button. The current configuration will be saved as a .bcf file in your host computer.

Administration > Configuration File > Import

OPAS

One-Plug-Auto-Service (OPAS) lets you collect system logs and other important device information, then save it to a computer or on a portable data storage device. OPAS automatically records a full report of system status, firmware version, event logs, setup, array configuration, and other essential information.

To save an OPAS information file to a portable data storage device, insert a USB flash drive into an available port and follow these steps:

1. Using a separate computer, attach a USB flash drive and create a folder on the flash drive named OPAS_files.
2. Remove the flash drive from the other computer and insert it in the USB port on the front of the DataGuard Appliance.
3. From the **Administration** tab, click the **OPAS** menu item.
4. Check the box marked **Enable USB OPAS**, then click the **Save** button.

To save an OPAS information file to a network location, follow these steps:

5. From the **Administration** tab, click the **OPAS** menu item.
6. Click the **Network OPAS** button and wait until the file is complete.
7. Click the **Download** button. If prompted, select a location for the file to be downloaded.

The compressed OPAS information file name uses the date and time of the download in the format *YearMonthDate* and an index number.

OPAS menu

Import/Export Users

To import user account information files, follow these steps:

1. From the **Administration** tab, click **Import Users**.
2. Click the **Browse** button (or Choose File button) and choose the previously saved file.
3. Click the **Submit** button.

An imported file can be created using a simple text program, or with Microsoft Word or Excel. For Excel, type for each user as follows: **username** (Column A), **password** (Column B), **quota** (Column C), **group name** (Column D), and **permission** (Column E).

For Word or plain text files, type the information with user name, password etc. separated by commas as in the syntax of the example below:

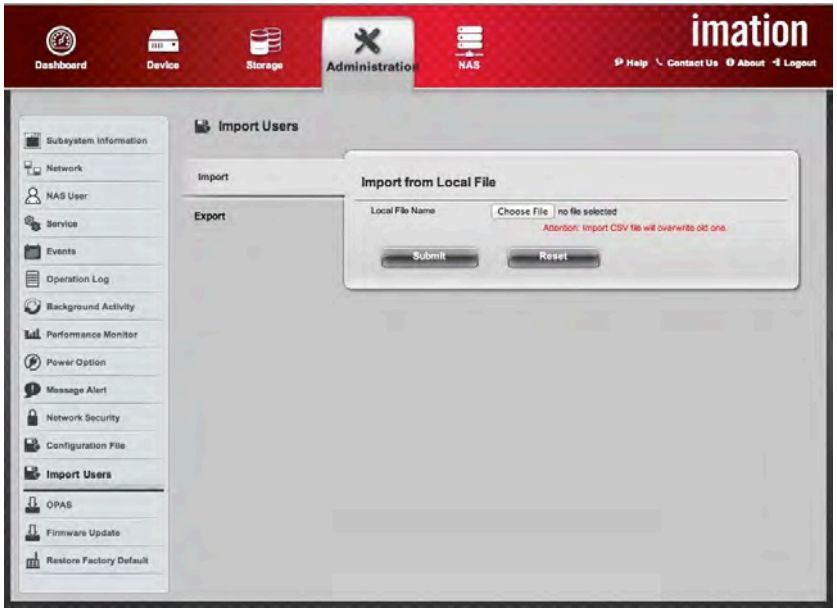
- ✓ user01,password,quota,group,permission
- ✓ user02,password,quota,group,permission
- ✓ user03,password,quota,group,permission

User quotas are in MB; a value of 0 (zero) means no quota is applied. The permission code is 0 = deny, 1 = read-only and 2 = read/write.

To export user account information files to your computer:

1. From the **Administration** tab, click **Import Users > Export**.
2. Click the **Submit** button.
3. Click the **Download** button. A prompt from your operating system should appear asking whether and where you want to download the file. Follow the instructions of the prompt to download the file to the target location.

Important
When you import user information files, the existing CSV file will be overwritten.

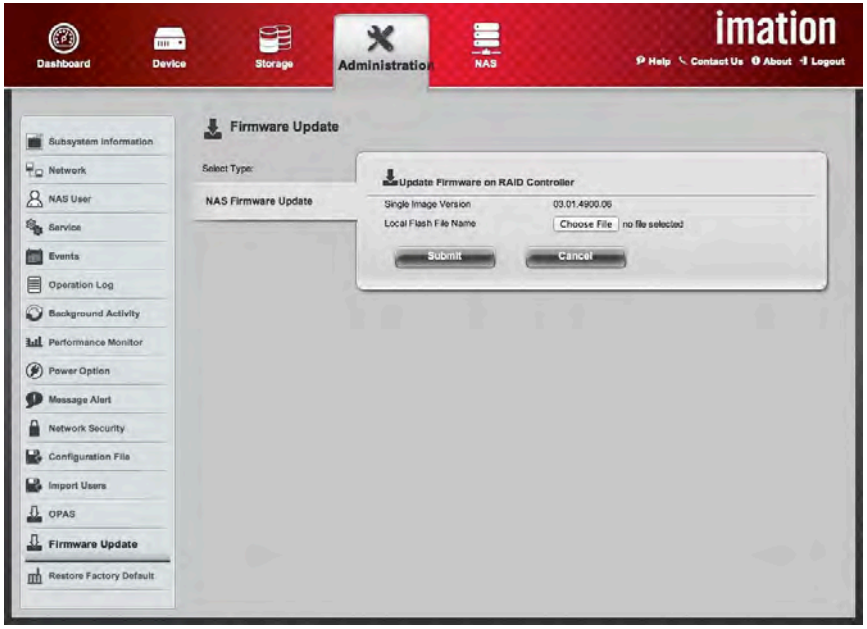


Administration > Import Users

Firmware updates

Before any firmware update, make sure you have the latest firmware image file on your desktop computer.

1. From the **Administration** tab, click the **Firmware Update** menu item. The Firmware Update panel will appear showing the current Image Version Number.
2. Click the **Browse** (or **Choose File**) button to locate the firmware image file, then click **Open**. The firmware image file will appear in the in the field.
3. Click the **Submit** button.
4. When the update is completed, you will see a message that tells you to reboot the subsystem. Click the **OK** button to restart the system.



Administration > Firmware Update

Warning
Do not power off the system during the update!

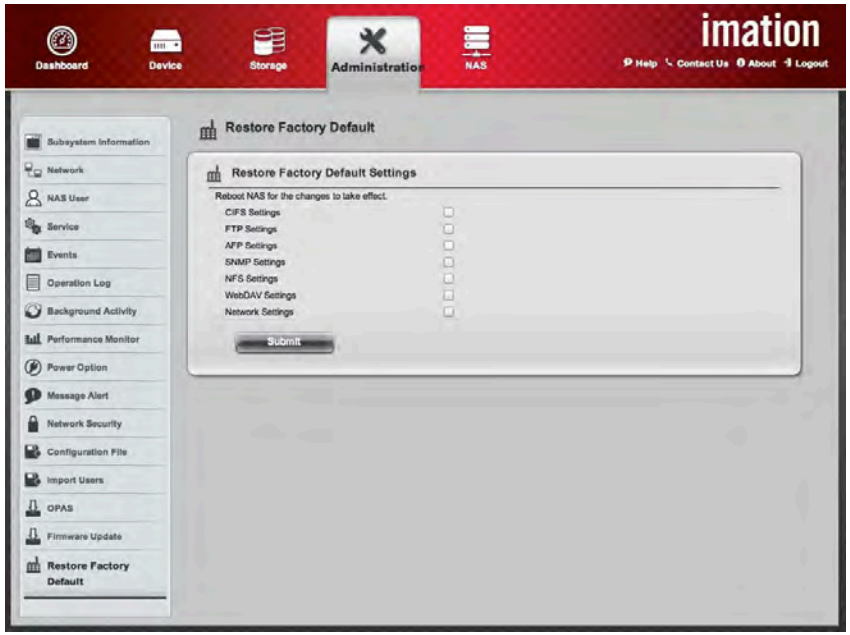
Restore Factory Default

This function allows you to restore any or all settings to their default values, including:

CIF Settings FTP Settings AFP Settings SNMP Settings
NFS Settings WebDAV Settings Network Settings

To restore the factory default settings:

1. From the **Administration** tab, click the **Restore Factory Default** menu item.
2. Check the boxes for each setting you want to reset to default value.
3. Click the **Submit** button.
4. Click **OK** to confirm, or click **Cancel** to leave the current settings intact.



Administration > Restore Factory Default

Caution
Use this feature only when required, and only on the settings that you must reset to default in order to set them correctly.

NAS Tab

Administrators can use the Backup menu in the DataGuard Management Interface to configure backup settings. Backup destinations can be locally connected hard drives or RDX cartridges, or online remote storage services such as DropBox, Amazon S3, and OpenStack. Administrators can also create Snapshot Backups and back up the DataGuard Appliance to an iSCSI target. You can also replicate one DataGuard Appliance to another.

To display the Backup menu, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item.
2. Select the Backup option you want by clicking one of these tabs: Snapshot Backup, Remote Backup, Local Backup, Amazon S3, Time Machine Backup, Backup to iSCSI, DropBox, OpenStack Object Storage, or RDX Backup.

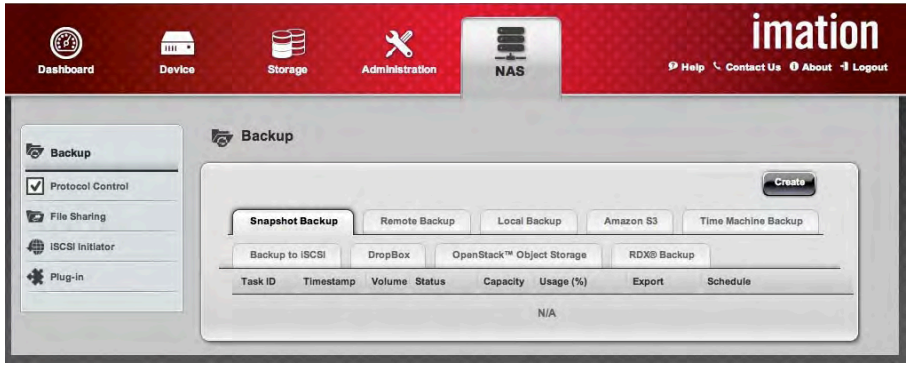
Snapshot Backup

1. From the **NAS** tab, click the **Backup** menu item, then click the **Snapshot Backup** folder tab.
2. Click the **Create** button to display the **Create Snapshot** menu.
3. Choose the **Volume** from which to take a Snapshot.
4. Enter a **Snapshot Size** or use the default (the maximum available); this must be at least 1.0 GB.

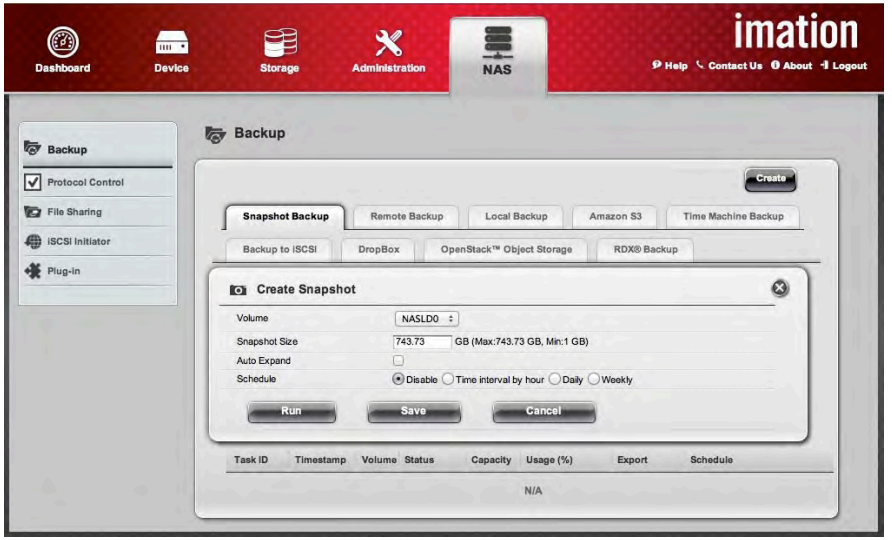
- **Auto Extend**: (Optional) Click to check the box that enables the function to use this feature, otherwise leave it unchecked.
- **Schedule***:* (Optional) Choose the schedule option and configure the desired schedule for Snapshot backups, Disable, Time interval by hour, Daily, or Weekly. Default = Disable (no Snapshot is taken).

5. When done, click the **Save** button to save the settings, or click the **Run** button to save the settings and execute the backup immediately.
6. Once the Snapshot backup configuration is created, the following options are available (move your pointer over the option and click).

✓ Recovery: Click to restore the data volume using the Snapshot.
✓ Export: Click to export the Snapshot to the share folder.
✓ Settings: Click to change the settings of the backup configuration.
✓ Delete: Click to delete the backup configuration.



NAS > Backup



NAS > Backup > Create Snapshot

Remote Backup (Client)

A remote data backup can be made from one DataGuard Appliance (Client) to another (Server). Follow these steps to create a Client backup:

1. From the **NAS** tab, click the **Backup** menu item, then click the **Remote Backup** folder tab.
2. Click the **Create** button and complete the required settings in the **Create Remote Backup** menu. Refer to the table at right for descriptions.
3. Select a schedule type for the backup.
4. When done, click the **Run** button. The new backup schedule is applied. You can click the **Test** button to test the server before applying the settings.
5. To change the configuration setting of a scheduled remote backup, move your pointer over the listed configuration to reveal the **Settings** icon and click on it to display the configuration settings menu.

Remote Backup (Server)

To serve as a backup destination, a DataGuard Appliance must be configured as a backup server. To perform a remote data backup using another DataGuard Appliance, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item, then click the **Remote Backup** folder tab.
2. Click the **Backup Server Setting** button and complete the required settings. Refer to the table at right for descriptions.
3. When you are finished, click the **Save** button to enable the server.

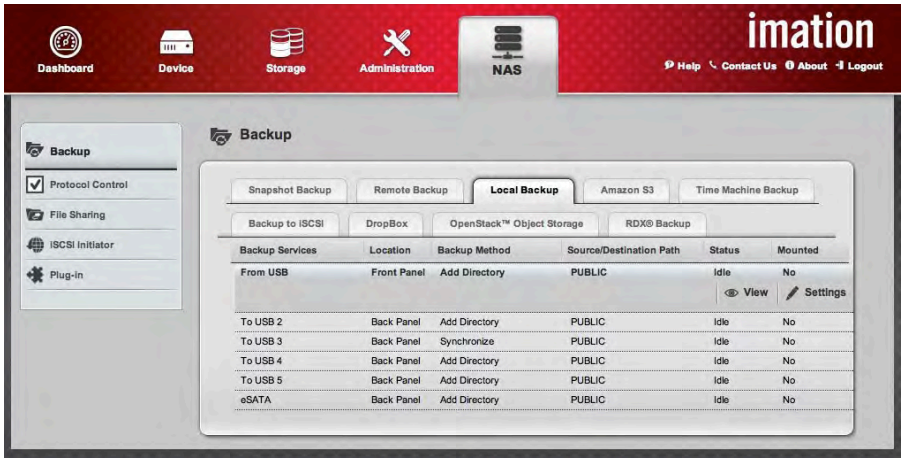
Configure the following settings for Remote Backups:

Setting	Description
Source Path	Click to select the folders to back up.
Destination Path	Enter the destination for the backup.
IP Address	Enter the IP address of the remote backup server.
Allow IP	Enter the IP addresses of data sources to allow backups from those clients.
Port	Enter the port number for the remote backup server.
User Name	Enter the user name to log in to the remote backup server.
Password	Enter the password to log in to the remote backup server.
Enable SSH	Select this option if the server requires SSH.
Snapshot	If Snapshot is disabled, the data backup can fail if data is written to or deleted from the DataGuard Appliance. The Snapshot will freeze the file system when the data backup will begin, so that changes to the data can be tolerated while the backup is in process. Any changes to the data that occur after the snapshot will not be included in the data backup. Enable this feature if the DataGuard Appliance will be used during remote backup.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables remote backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)
Backup Method	**Add Directory**—Creates a new folder and transfers the contents to this folder. The new folder is named according to the Hostname and date of creation. **Copy**—In the target folder, this overwrites existing folders with identical names but does not effect other folders that might be present. **Synchronize**—In the target folder, this overwrites existing folders with identical names and removes any other folders so that the data contents are identical on the client and destination folder.

Local Backup

The DataGuard Appliance can make data backups to local drives connected by USB or eSATA. Configure the following settings for local backups:

Setting	Description
Backup Method (choose one)	**Add Directory**—Creates a new folder and transfers the contents to this folder. The new folder is named according to the Hostname and date of creation. **Copy**—In the target folder, this overwrites existing folders with identical names but does not effect other folders that might be present. **Synchronize**—In the target folder, this overwrites existing folders with identical names and removes any other folders so that the data contents are identical on the client and destination folder.
Destination Path/ Folder Name	Choose a folder or folders to back up from or a destination folder to backup to by clicking to check the folder or folders in the list.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables remote backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)



NAS > Backup > Local Backup

Important

Carefully consider the Backup Method used when backing up to or from a USB device so that data you want to keep is not overwritten.

Backup to USB

USB Ports 2–5, on the back panel of the DataGuard Appliance, can be used for backing up local folders to a suitable USB storage device. USB Port 1 on the front panel can be used to restore data to the DataGuard Appliance from a USB storage device.

To configure data backup to a USB direct attached system, follow these steps:

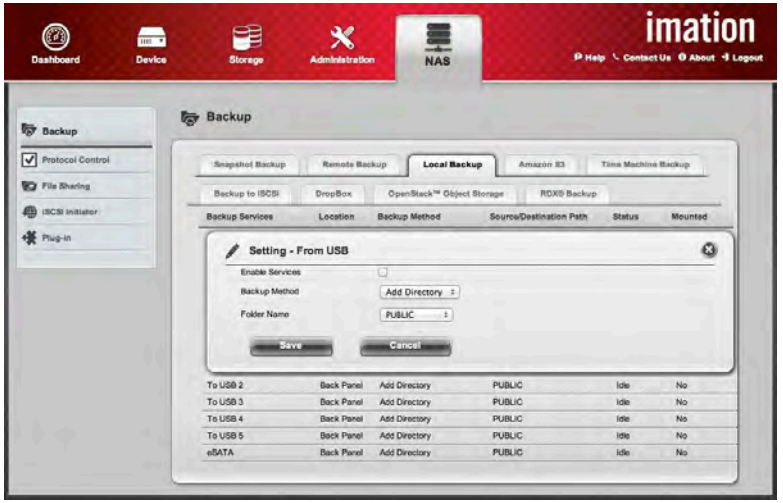
1. From the **NAS** tab, click the **Backup** menu item, then click the **Local Backup folder** tab.
2. Move your pointer over the listed USB attached device that will receive the backup data and click on **Settings**. For USB devices, use the appropriate “To USB” device listed.
3. Choose a **Backup Method**. Make sure you understand the available options Add Directory, Copy and Synchronize, and how each option affects the data on the destination device.
4. Select the schedule type you want for the backup.
5. When done, click the **Run** button new begin backup, or **Save** to begin according to the configured schedule. The new backup schedule is in effect.
6. To change the configuration setting of a scheduled USB local backup, move your pointer over the listed configuration to reveal the **Settings** icon and click on it to display the configuration settings menu. Click **View** to display the current settings without configuration options.

Restore from USB

To configure data back up from a USB direct attached system, follow these steps:

1. Click **NAS** tab > **Backup** > **Local Backup** tab.
2. Move your pointer over the listed “From USB” device that is the source of the data to backup and click on **Settings**.
3. Choose a **Backup Method**. Make sure you understand the available options Add Directory, Copy and Synchronize, and how each option affects the data restored to the DataGuard Appliance.
4. Click to select the **Enable Services** box to allow the backup to occur using the chosen method.
5. Choose the destination folder for the backup.
6. Click the **Save** button. The NAS is now ready to receive the data backup as configured when the process is launched.
7. Click the **One-Touch Backup** button on the front panel to initiate restoration through USB Port 1.
8. To change the configuration setting of a scheduled USB local backup, move your pointer over the listed configuration to reveal the **Settings** icon and click on it to display the configuration settings menu. Click **View** to display the current settings without configuration options.

NAS > Backup > Local Backup > Backup to USB



NAS > Backup > Local Backup > Restore from USB

Backup to eSATA

To configure data back up to a direct attached system via the eSATA port, make sure the eSATA device is connected and powered on, then follow these steps:

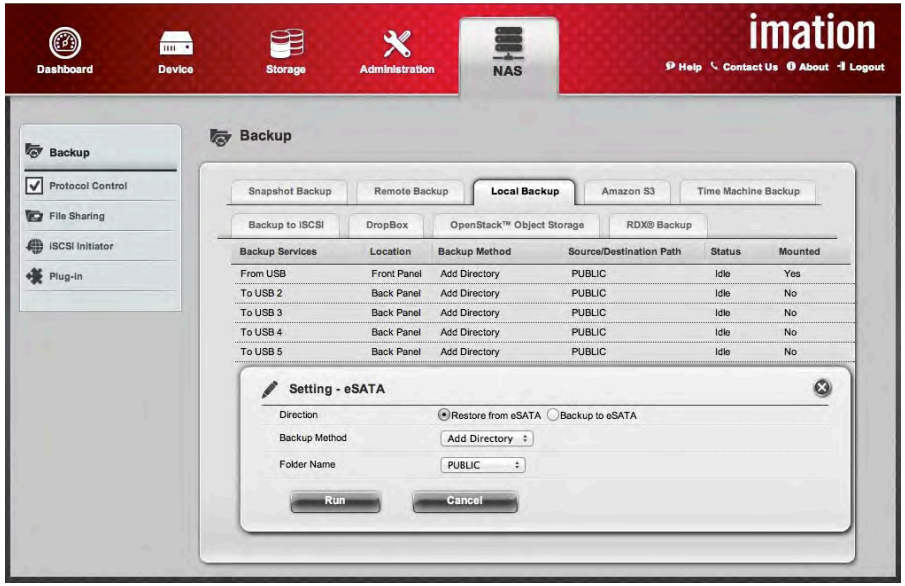
1. From the **NAS** tab, click the **Backup** menu item, then click the **Local Backup** tab.
2. Move your pointer over the **eSATA** row and click on **Settings**.
3. Click the **Backup to eSATA** radio button.
4. Choose a **Backup Method**. Make sure you understand the available options Add Directory, Copy and Synchronize, and how each option affects the data on the destination eSATA device.
5. Select the schedule type you want for the backup.
6. When done, click the **Run** button to begin backup immediately, or **Save** to begin according to the configured schedule. The new backup schedule is in effect.

Restore from eSATA

To launch a data restoration from an attached eSATA device, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item, then

1. Click **NAS** tab > **Backup** > **Local Backup** tab.
2. Move your pointer over the **eSATA** row and click on **Settings**.
3. Click the **Restore from eSATA** radio button.
4. Choose the **Backup Method** used to manage the data transfer. Make sure to understand the available options Add Directory, Copy and Synchronize and how each option deals with data on the NAS.
5. Click the **Run** button to begin the data restoration process.



NAS > Backup > eSATA

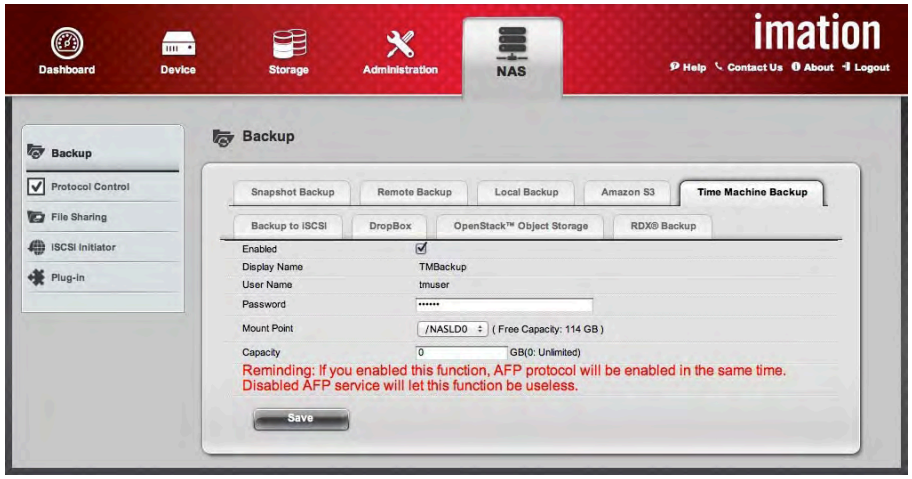
Backup using Mac OS Time Machine

The DataGuard Appliance can be used with Time Machine, a backup utility included with Mac OS X 10.5, 10.6 and 10.7. To create a Time Machine backup, follow these steps:

1. Make sure your Mac is running and connected to the same network as the DataGuard Appliance.
2. Set up a folder to be used for Time Machine backups.
3. From the **NAS** tab, click the **Backup** menu item, then click the **Local Backup** folder tab.
4. Check the **Enabled** box.
5. Enter a **User Name** for the account that will use the DataGuard Appliance for Time Machine backup.
6. Enter the **Password** of the user account.
7. Choose a **Mount Point** from the pull-down menu. This defines a dedicated space used for Time Machine backups.
8. Click the **Save** button.

The newly mounted drive should appear on the desktop, and in the Finder labeled with the user account login user name.

For instructions on configuring Time Machine, refer to Apple documentation.



NAS > Backup > Time Machine Backup

Important

In order to use Time Machine, you must create a user account for the system that uses the DataGuard Appliance for backup.

Important

Use RAID 1 or higher for drives used for Time Machine backup to insure against loss of data.

Do not use RAID 0 for Time Machine backup since the failure of any physical hard disk drive means all data is lost.

Backup to Amazon S3

An administrator can back up the contents of the DataGuard Appliance to an Amazon Simple Storage Service (Amazon S3) server with an Amazon account. To create an Amazon S3 backup, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item, then click the **Amazon S3** folder tab.
2. Click the **Create** button and complete the required settings in the **Create Remote Backup** menu.
3. Select one of the schedule types you want for the backup solution.
4. When done, click the **Run** button. The new backup schedule is applied. You can click the **Test** button to test the server before applying the settings.
5. To change the configuration setting of a scheduled S3 backup, move your pointer over the listed configuration to reveal the **Settings** icon and click on it to display the configuration settings menu.

Configure the following settings for Amazon S3:

Setting	Description
Local Path	Click to select which folders to back up.
Direction	Select Download (from Amazon S3 to device) or Upload (from device to Amazon S3)
Access Key	Enter the Access key for the Amazon S3 server.
Private Key	Enter the Private key for the Amazon S3 server.
Retries Number	Enter the number of attempts to retry if the negotiation fails.
Incremental Backup	Select this option to add updated files only.
Synchronized Backup	Select this option to delete extra files while synchronizing.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables Amazon S3 backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)

NAS > Backup > Amazon S3

Backup to DropBox

An administrator can back up the contents of the DataGuard Appliance to a DropBox server. To create a DropBox backup, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item, then click the **DropBox** folder tab.
2. Click the **Create** button and complete the required settings in the **Create DropBox Backup** menu.
3. Enter the DropBox account information (email address and password)
4. Select the schedule type you want for the backup.
5. When done, click the **Run** button to begin backing up immediately. You can click the **Test** button to test the server before applying the settings. Click **Save** to save the schedule and account settings.

After you run or test a DropBox backup, a new folder will appear within your DropBox folder. This folder contains the contents of the specified Home folder. To restore the data, open the folder and retrieve the files as you would with any data stored in your DropBox folder.

Configure the following settings for DropBox Backup:

Setting	Description
Direction	The direction of the backup is upload. DropBox Backup will backup the user's Home folder by uploading the data to the DropBox server. Note that the DropBox should have enough storage space available to accommodate the backup.
DropBox Email	The user enters the email account used for the DropBox account.
DropBox Password	The user enters the password used for the DropBox account.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables DropBox backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)

NAS > Backup > DropBox

Backup to OpenStack

An administrator can back up the contents of the DataGuard Appliance to an OpenStack Object Storage cloud.

To create an OpenStack backup, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item, then click the **OpenStack Object Storage** folder tab.
2. Click the **Create** button and complete the required settings in the **Create OpenStack Backup** menu.
3. Determine what local folder or folders are used for backup or transfer in the **Local Path** selection menu. Click to check the selection box for folders used for backup.
4. Select the **Direction** of the data transfer (Upload or Download)
5. Enter the URL of the **Authentication Server** for the account.
6. Enter the OpenStack **User Name** and **API Key**.
7. OpenStack backup options available include Incremental Backup and Synchronized Backup (see description in table).
8. Select the schedule type you want for the backup.
9. When done, click the **Run** button to begin backing up immediately. You can click the **Test** button to test the server before applying the settings. Click **Save** to save the schedule and account settings.

Configure the following settings for OpenStack Backup:

Setting	Description
Local Path	Click to select the folders to back up to OpenStack, or choose the folder to transfer data from the OpenStack cloud.
Direction	Select Download (from OpenStack to device) or Upload (from device to OpenStack)
Authentication Server	The URL used for the OpenStack account connection.
User Name	The OpenStack account user name. This is created when the OpenStack account is set up.
API Key	This is the secret key used for the account. The user should obtain this when the account is set up.
Incremental Back-up	An incremental backup is used in order to preserve data without creating multiple copies, that is, without duplication of existing backups. Backups completed in increments, taking into account what has been backed up in the previous incremental backup sessions. Initially and full backup is completed, and subsequent backups will take place backing up only data folders that have changed since the previous backup.
Synchronized Backup	Overwrite existing folders with identical names and removes any other folders so that the data contents are identical on the client and destination folder.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables OpenStack backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)

Backup to RDX

The RDX drive is ideal for secure and rapid transfer of large amounts of data for backup or use on another systems. RDX cartridges can be transported to other backup systems or supporting devices. Follow the instructions in this section to either restore data that has been previously backed up, or to back up data to RDX.

To configure data back up to a USB direct attached system, follow these steps:

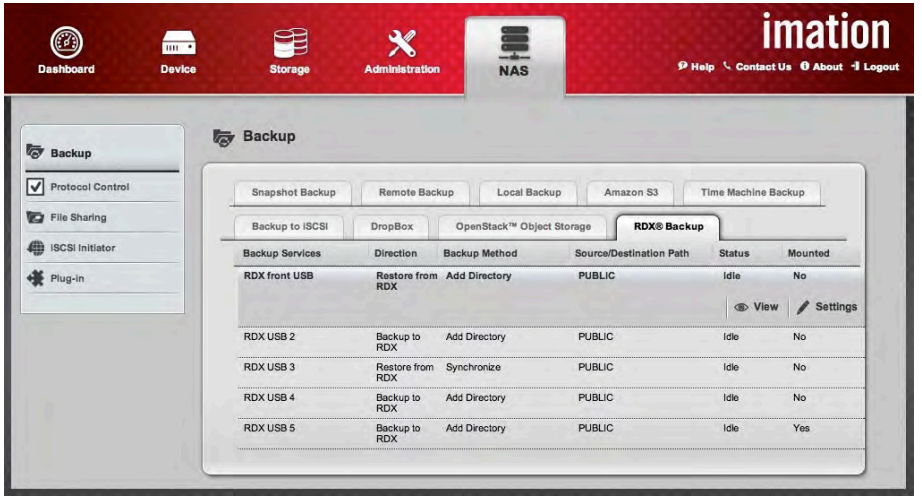
1. From the **NAS** tab, click the **Backup** menu item, then click the **RDX Backup folder** tab.
2. Move your pointer over the listed options for RDX and click on **Settings**.
3. Select a **Backup Method**—Add Directory, Copy, or Synchronize (see table at right)
4. Select the schedule type you want for the backup.
5. When done, click the **Run** button new begin backup, or **Save** to begin according to the configured schedule. The new backup schedule is in effect.

Restore from RDX

To configure data back up from a USB direct attached system, follow these steps:

1. From the **NAS** tab, click the **Backup** menu item, then click the **RDX Backup folder** tab.
2. Move your pointer over the listed options for RDX and click on **Settings**.
3. Click the **Restore from RDX** radio button.
4. Choose the **Backup Method** used to manage the data transfer.
5. Select a destination folder for the restored data.
6. Click the **Run** button to begin the data restoration process.

Important
The USB port on the front panel (USB1) as well as USB2 and USB3 ports use a slower version of the USB specification. Keep this in mind if you are transferring large amount of data to or from RDX.



RDX Backup function for USB ports

Configure the following settings for RDX Backup:

Setting	Description
Backup Method (choose one)	Add Directory—Creates a new folder and transfers the contents to this folder. The new folder is named according to the Hostname and date of creation. Copy—In the target folder, this overwrites existing folders with identical names but does not affect other folders that might be present. Synchronize—In the target folder, this overwrites existing folders with identical names and removes any other folders so that the data contents are identical on the client and destination folder.
Destination Path/ Folder Name	Choose a folder or folders to back up from or a destination folder to backup to by clicking to check the folder or folders in the list.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables OpenStack backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)

Backup to iSCSI

An iSCSI backup will create a complete copy of the logical drive, including the RAID configuration. Data can be restored to a DataGuard Appliance from an iSCSI backup without creating a new logical drive and file system.

To recreate a logical drive and data, the DataGuard Appliance must have the same number of unconfigured hard disks available as were present when the iSCSI backup was created. The DataGuard Appliance must also be configured as an iSCSI initiator for the device that it will use for iSCSI Backup.

To configure the NAS as an iSCSI initiator, see “iSCSI Initiator” on page 78. To review the process used to restore a logical drive from the iSCSI target, see “iSCSI Restore LD Process” on page 73.

To create an iSCSI Backup of a logical drive, follow these steps:
From the **NAS** tab, click the **Backup** menu item, then click the **Backup to iSCSI** folder tab.

1. Click the **Create** button to open the **Create iSCSI Backup** menu.
2. Enter the IP address of an iSCSI device configured for use by the DataGuard Appliance; it is also possible to change the port here. Click the **Next** button.
3. The new menu lists the IP address and port you entered for the iSCSI device. The iSCSI name (IQN) appears here. If CHAP authentication is used, enable it by checking the **CHAP** option box, then type the **User Name** and **Password** used for CHAP. Click the **Next** button.
4. In the new menu, information entered previously is listed including the IQN and CHAP status (ON or OFF). If multiple LUN are mapped for use on the iSCSI devices, choose the one to use for the configured backup. It is a good idea to enable a **Snapshot** to be saved to the iSCSI, especially if a write activity will take while the backup is in progress. Check the Snapshot box to enable a Snapshot backup to iSCSI.
5. Select one of the schedule types you want for the backup solution.
6. When done, click the **Run** button to begin backing up immediately. Click **Save** to save the schedule and account settings.

Configure the following settings for iSCSI Backup:

Setting	Description
Backup Server	IP address of iSCSI device. Make sure the NAS is configured as an iSCSI initiator before running the backup.
Port	The port used for iSCSI connection.
CHAP	Enable if using CHAP for authentication.
User Name	If CHAP is used, enter the User Name.
Password	If CHAP is used, enter the Password.
Snapshot	Select this option if you want to upload snapshot of backup to the server.
Schedule	Choose the schedule option and configure the desired schedule for backups: Disable—Disables iSCSI backup • Time interval by hour—Backup is done at the hourly interval you choose from the drop-down menu • Daily—Backup is scheduled at the time of day you choose from the drop-down menus • Weekly—Backup is scheduled at the day of the week, at the time of day you choose from the drop-down menus. • Default—Disabled (no backup is scheduled)

iSCSI Restore LD Process

The iSCSI Backup function is used to backup an entire logical drive with its RAID configuration intact. The restore function for iSCSI Backup will only work if the physical drives where the logical drive will be replaced meet two important conditions. First, the drives must not be configured, that is, there cannot be an array or logical drive present on the physical drives. And second, the drives must be at least as large as the drives that contained the original logical drive in the iSCSI Backup.

To recover a logical drive that has failed, use the Restore function of the iSCSI Backup. In order to complete a recovery, the DataGuard Appliance with the failed logical drive must be populated with unconfigured hard drives in the same number and size as when the iSCSI Backup was created.

If the failed logical drive or the array in which it was created are still present, the restore function will abort because an LD is detected. In order to reuse the same physical drives, assuming they remain in good working condition, it will be necessary to first remove the existing array made up of the physical drives. Alternatively, the original physical drives can be replaced with new drives that are the same size or larger.

To restore a failed logical drive, make sure the conditions discussed above apply, and follow these steps:

1. Click **NAS** tab **> Backup > Backup to iSCSI** tab.
2. Enter the IP address of the remote iSCSI device used for backup and enter the Port used. These values should be the same are those entered in the iSCSI Backup configuration. Click **Next** to continue.
3. Find the iSCSI Name of the device in the pull-down menu. If CHAP has been configured, click the **CHAP** option box to enable it and enter the **User Name** and **Password** in the spaces provided. Click **Next** to continue.
4. If more than one LD are backed up on the iSCSI device it will be necessary to choose the LUN ID of the one that is being restored. Use the **LUN ID** pull-down menu to select it. Click **Next** to continue.
5. Choose the Source from the pull-down menu if there are more than one iSCSI devices with backups.
6. Click on the **Restore** button. The restore process will commence after a brief negotiation process. When both systems are ready, the restore will begin. The length of time needed to complete the process depends on the size of the LD and the amount of data stored on it.

Important: If the restore process fails, check to make sure that the NAS has unconfigured (no file system, no LD, no array) hard drives available and that the drives are at least as large as the original drives they replace. The restoration process will abort if the array or logical drive that failed is still present on the NAS. See “Physical Drive” on page 26 for instructions on how to view hardware information about the disks installed. See “Manage Disk Arrays” on page 32 for array information. See “Logical Drive Management” on page <?> for logical drive information.

Protocol Control

Control and Setting

1. From the **NAS** tab, click the **Protocol Control** menu item.
2. In the **Protocol Control** list, move your pointer over the protocol option you want and click the **Enable/Disable** button to turn the feature ON/OFF. The protocols include:
   - Windows (CIFS)
   - UNIX/Linu
   - Printer Server
   - DFS
   - FTP Sharing
   - Mac AFP
   - WebDAV
3. To change the protocol settings, move your pointer over the protocol option and click the **Settings** button to configure the advanced settings.

Warning
Changes to the Protocol Control will interrupt all connections. Make sure no connections are active before applying a change.

Windows CIFS

The Common Internet File System (CIFS) Protocol is a dialect of the Server Message Block (SMB) Protocol known as Microsoft SMB Protocol in Windows. CIFS is enabled by default. To disable CIFS, click the **Cancel** button. Disabling the CIFS does not change the saved configuration settings.
To configure Windows CIFS:

1. From the **NAS** tab, click the **Protocol Control** menu item.
2. Move your pointer to expand the **Windows CIFS** row of the **Protocol Control** list and click on **Settings**.
3. Click **Enable Services** (enabled by default) to enable CIFS as configured in this menu.
4. Enter the **Computer Name** and **Computer Description** used for the DataGuard Appliance. (The default name and description used are the name are configured in the Network settings menu.)
5. Choose the type of membership for the DataGuard Appliance.
6. If the DataGuard Appliance is configured as a member of a Windows Workgroup, enter a **Workgroup** name in the entry field provided (default = *WORKGROUP*).
   a. If the DataGuard Appliance is configured as a member of an **AD Domain (**Active Directory Domain), enter the **Domain Controller**, **Administrator Account**, and **Administrator Password** in the entry fields displayed and choose the read/write permission setting.
7. Click the **Save** button to apply and save the settings.

FTP Sharing

To configure FTP Sharing:

1. Click **NAS** tab > **Protocol Control**.
2. Move your pointer to expand the **FTP Sharing** row of the **Protocol Control** list and click on **Settings**.
3. Click **Enable Services** (enabled by default) to enable FTP as configured in this menu.
4. Enter the **Command Port**.
5. Enter a range of **Passive Ports** used for FTP clients.
6. Choose the **Client Coding Type** for the language preference (choose *English (Unicode), Japanese, Simplified Chinese, Traditional Chinese* or *Korean)*.
7. Choose the **Protocol Type** [*Standard FTP, FTP over SSL (Explicit), FTP over SSL (Implicit, Command Port 990, SFTP*].
8. Click the **Enable Anonymous** (enabled by default) to disable or enable anonymous FTP login.
9. Type a number for the maximum number of concurrent FTP connections allowed the **Maximum Connection** field. (default = 256)
10. Enter a limit for bandwidth in the **Maximum Download/Upload Rate** entry fields. (0= no limit)
11. Click the **Save** button to apply and save the settings.

UNIX/Linux (NFS) Service

Use the UNIX/Linux Settings menu to configure and activate the UNIX and Linux NFS service for the DataGuard Appliance. When this is enabled and running, UNIX and Linux computer users can access and use the DataGuard Appliance from the network. If you are going to set up a network drive for a UNIX or Linux system, this must be enabled.
To configure FTP Sharing:

1. Click **NAS** tab > **Protocol Control**.
2. Move your pointer to expand the **UNIX/Linux** row of the **Protocol Control** list and click on **Settings**.
3. Click **Enable Services** (enabled by default) to enable UNIX/Linux service.
4. (*Optional*) UNIX/Linux service inlcudes the option of joining an NIS (Network Information Service) domain. To use NIS domains, click to check the **Enable NIS** and enter the NIS Domain Name.
5. Click the **Save** button to apply and save the settings.

MAC AFP

Use the Mac AFP Settings menu to configure and activate Apple Filing Protocol service to enable Mac users to access and use the DataGuard Appliance from the network.
To configure Mac AFP:

1. Click **NAS** tab > **Protocol Control**.
2. Move your pointer to expand the **MAC AFP** row of the **Protocol Control** list and click on **Settings**.
3. Click **Enable Services** (enabled by default) to enable AFP service.
4. (*Optional*) Enter a **Login Message**. This message appears in the Welcome screen when logging in from a Mac client.
5. Click the **Save** button to apply and save the settings.

Printer Server

The embedded print server is disabled by default. This must be enabled to connect a network printer to the DataGuard Appliance with a USB cable.
To enable or disable :

1. Click **NAS** tab > **Protocol Control**.
2. Move your pointer to expand the **Printer Server** row of the **Protocol Control** list and click on **Settings**.
3. Click to check **Enable Services** (disabled by default) to enable printer service. Click the same box to remove the check mark to disable printer service.
4. Click the **Save** button to apply and save the settings.

WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) support for remote web content editing. It is enabled by default.
To enable or disable :

1. Click **NAS** tab > **Protocol Control**.
2. Move your pointer to expand the **WebDAV** row of the **Protocol Control** list and click on **Settings**.
3. Click to check **Enable Services** (enabled by default) to enable WebDAV. Click the same box to remove the check mark to disable WebDAV.
4. Click the **Save** button to apply and save the settings.

DFS

The DataGuard Appliance supports Distributed File DFS for Windows which is disabled by default. DFS allows for control of access to folders on the DataGuard Appliance by remote clients. To use DFS, it must first be enabled by clicking on the **Enable** icon. Once enabled, you can add client configurations. Follow the instructions below to configure NFS access.

Click **NAS** tab > **Protocol Control**.

5. Move your pointer to expand the **DFS** row of the **Protocol Control** list and click on **Add**.
6. In the Add client menu, Enter the **Storage** name (client name), the **Share Folder** allowed access to the client and the **Alias** of the client.
7. Click the **Save** button to apply and save the settings.
8. To view the list of clients configured for access, click on the **View** icon. Configurations can be deleted using this list.

File Sharing

When the new user/group is added, you have to complete the permission settings for each user/group to access the system. Use the File Sharing menu to change the permission settings for each share folder on a per user basis. This is also the menu used to create new share folders and to create a shared ISO folder within an existing shared folder.

To configure share settings for a folder on the DataGuard Appliance:

1. From the **NAS** tab, click the **File Sharing** menu item.
2. Move your pointer over the folder you want and click the **Share Settings** button.
3. Select the user/group you want and set an access option: Deny-Access, Read-Only, or Read-Write.
4. When done, click the **Save** button.

To create a new shared folder:

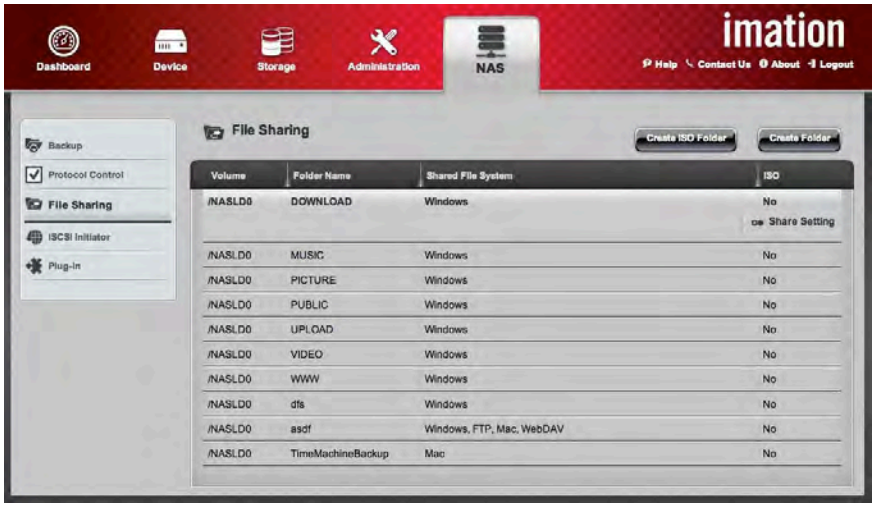
1. From the **NAS** tab, click the **File Sharing** menu item.
2. Click the **Create Folder** button.
3. Choose the **Volume** and type a name for the **Folder** and click the **Next** button.
4. Click on the option box(es) to select the base protocol for the folder (Windows/Mac/FTP/WebDAVor UNIX/LINUX) and click the **Next** button.
5. If the base protocol selected in the previous menu was Windows/ Mac/FTP/WebDAV, click on the option box(es) to specify the supported protocols (Windows, Mac, FTP, or WebDAV; default = all enabled) and configure user permissions. For UNIX/LINUX folders, it is necessary to specify an IP address on the local network with read/write permission. If both UNIX/LINUX and Windows/MAC are supported, specify the IP address in this or the next menu screen. Click the **Next** button to continue.
6. Review the folder configuration settings and click on **Submit** to create the new folder

To create a folder for an ISO image:

1. From the **NAS** tab, click the **File Sharing** menu item.
2. Click the **Create ISO Folder** button to add a folder for ISO file sharing:

- Enter the **Source Folder**, **ISO Image File** and **Folder Name**, and then click the **Next** button.
- Select the protocol as Windows/FTP or UNIX/LINUX, and then click the **Next** button.
- In the **Permission Setting** field, set the privilege for the users to access the folder by selecting: Deny-Access, Read-Only, or Read-Write. Click the **Next** button.
- When done, click the **Submit** button.

3. In the **File Sharing** list, move your pointer over the item and clicking the Share Setting button to change the sharing settings.



NAS > File Sharing

iSCSI Initiator

Use the iSCSI Initiator feature to use the DataGuard Appliance as an initiator. This must be done before performing an iSCSI Backup or restore. To use the iSCSI Initiator function, follow the steps listed below. Keep in mind that the DataGuard Appliance must have at least one logical drive acting in the role of a NAS (i.e. LDType = NAS).

1. From the **NAS** tab, click the **iSCSI Initiator** menu item, then click the **Create** button to open the **Create iSCSI Initiator** menu.
2. Enter the IP address of the iSCSI target device. If CHAP authentication is used, enable it by clicking to check mark the **CHAP** option box, type the **User Name** and **Password** used for CHAP. Click the **Next** button to proceed.
3. The new menu lists the IP address and port you just entered for the iSCSI device. The iSCSI name (IQN) should appear listed here as well. Enter an **Alias Name** for the target. The alias name functions as the name of a folder created in the NAS (initiator) file system. Click the **Save** button. The NAS should now be connected to the target. If there is no file system on the target drive, it will be necessary to format it before it can be "mounted" or used in the NAS initiator file system.
4. In the main iSCSI Initiator menu, hold your pointer over the listed target device to reveal the buttons to **Connect**, **Format** or **Delete**. If the target has been formatted, use the **Connect** button to mount the target on the home DataGuard Appliance (initiator). **If there is no file system on the target, it will be necessary to format the drive**. See example of an unformatted target displayed in the iSCSI Initiator menu.

   ✓ If the drive is not formatted, click the Format button. All data on the drive will be written over and lost when formatted.

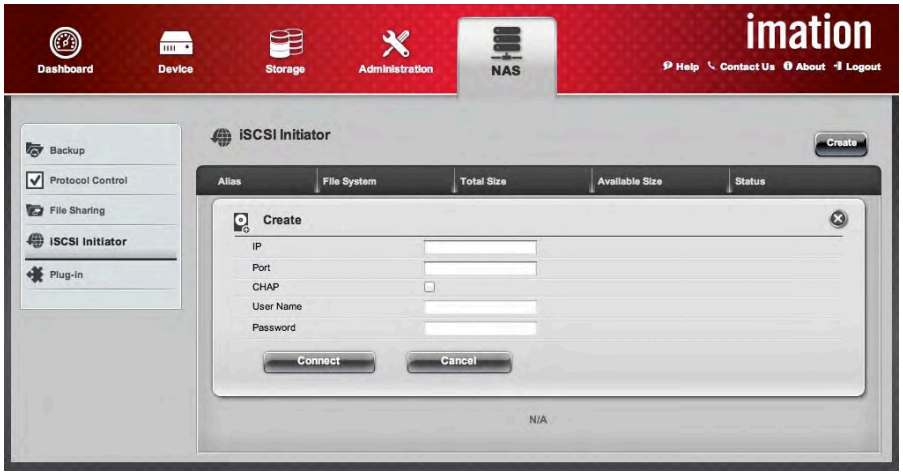
   ✓ To connect or reconnect to the Target, click the Connect button.

   ✓ To remove the Target from the NAS file system, click the Delete button.

   ✓ The newly created iSCSI session will be listed in the iSCSI menu (click Device > iSCSI > Session tab) for the initiator device. The added storage can be used for backup of the NAS (see "Backup to iSCSI" on page 72); or use it as additional storage for NAS users. Use the Web File Manager to configure user permissions. The iSCSI connection supports use of AFP, DFS, Samba and FTP for client connections.

After establishing the iSCSI target connection, a folder appears in file system of the initiator with the name entered in the Alias Name field. This folder can be configured just like any other folder using the Web File Manager plug-in to assign read/write access permissions for users.

Important
An iSCSI target that has not been formatted is indicated if there is no file system present and 0 bytes of free space.



NAS > iSCSI Initiator > Create

Plug-ins

Plug-in services provide enhanced server functions. The Web File Manager is pre-installed to help you create and manage files on the DataGuard Appliance. Web File Manager is permanently embedded in the firmware; it can be stopped but cannot be removed. To view the available function icons for Web File Manager, move your pointer to the row where it is listed and click on the **Open** icon.

NAS > Plug-in > Web File Manager